

The Maine Through Year System and Technology Guide

**2024–2025 Maine Through Year Assessment
Reading and Mathematics**

Table of contents

- Part 1—IT staff readiness checklist** 3
- Part 2—Online readiness tools** 4
 - System requirements check 4
 - Secure browser download 4
 - School capacity calculator 4
 - System check test 5
- Part 3—System requirements** 6
 - Requirements for Acacia testing online 6
 - Acacia management and reporting system requirements 7
- Part 4—Network requirements** 8
 - Network connections 8
 - Bandwidth 8
 - Wireless access points 10
 - Network diagnostic tools 11
 - Network configurations 12
 - Virtualization guidelines 13
- Part 5—The NWEA State Solutions Secure Browser** 15
 - About the NWEA State Solutions Secure Browser 15
 - Windows installation and management 15
 - Chromebook installation and management 21
 - macOS installation and management 25
 - iOS installation and management 30
 - Updating the partner code 33

Part 1—IT staff readiness checklist

	Action Item	Timeline	Resource
<input type="checkbox"/>	Review system maintenance windows	Yearly	System Maintenance Windows on NWEA Connection
<input type="checkbox"/>	Verify network meets requirements and conduct network diagnostics.	Can begin immediately	Network requirements on page 8 Note: Some requirements have been updated for 2024–2025
<input type="checkbox"/>	Verify testing devices meet minimum hardware and software requirements.	Can begin immediately	System requirements on page 6 Note: Some requirements have been updated for 2024–2025
<input type="checkbox"/>	Uninstall the previous year's version of the NWEA State Solutions Secure Browser on Macs, PCs, and Chromebooks. iOS apps update automatically	3–4 weeks before testing begins	The NWEA State Solutions Secure Browser on page 15
<input type="checkbox"/>	Install the correct version of the NWEA State Solutions Secure Browser on all testing devices.	3–4 weeks before testing begins	The NWEA State Solutions Secure Browser on page 15 Note: The testing browser has been updated for 2024–2025
<input type="checkbox"/>	Windows: Disable Fast User Switching.	2–3 weeks before testing begins	Disable Fast User Switching in Windows on page 19
<input type="checkbox"/>	Ensure that all applications not identified as necessary by the technology staff are uninstalled from testing computers. Shut down any automatic updates during the testing window.	1–2 weeks before testing begins	
<input type="checkbox"/>	Ensure staff availability to assist with technical issues during the testing window.	Ongoing throughout the testing window	

Part 2—Online readiness tools

NWEA has online readiness tools to help schools plan for testing. The Online Readiness Tools website has the following tools available:

- System requirements check
- Secure browser download
- System check test to determine the maximum number of simultaneous testers your network can accommodate
- School capacity calculator

The Online Readiness Tools website is available at <https://securebrowser.state.nwea.org>.

System requirements check

At the top of the Online Readiness Tools page, your operating system and browser version are listed. Compare this with the system requirements in this document at [Requirements for Acacia testing online](#) on page 6, or download the System Requirements Guide, linked on the Online Readiness Tools page.

Secure browser download

Installers (or links to the appropriate app download site) for the NWEA State Solutions Secure Browser are available for each supported platform.

School capacity calculator

The school capacity calculator helps plan for the test administration. It is used to determine the following:

- Maximum student capacity
- Minimum required computers
- Minimum test sessions per day
- Minimum required days of testing

Maximum student capacity

To determine the maximum student capacity, enter the number of computers, the number of test sessions available per day, and the number of days allowed for testing. Select the **Calculate** button and the system will provide the maximum student capacity for testing.

Minimum required computers

To determine the minimum required computers, enter the total number of student testing administrations, the number of test sessions available per day, and the number of days allowed for testing. Select the **Calculate** button and the system will provide the minimum number of computers required for testing.

Minimum test sessions per day

To determine the minimum test sessions per day, enter the number of computers, the total number of student testing administrations, and the number of days allowed for testing. Select the **Calculate** button and the system will provide the minimum number of sessions needed each day for testing.

Minimum required days of testing

To determine the minimum required days of testing, enter the number of computers, the total number of student testing administrations, and the number of sessions available per day. Select the **Calculate** button and the system will provide the minimum number of days needed for testing.

System check test

The system check test performs a speed test on your network, then calculates the maximum number of simultaneous test takers that can be supported by your network at that speed. Run this test during peak usage to assess the available bandwidth and network traffic. Local bandwidth will vary with usage and traffic levels, so it should be run when usage is similar to usage on a testing day.

Part 3—System requirements

Requirements for Acacia testing online

You can verify that you have the most up-to-date system requirements throughout the year at <https://securebrowser.state.nwea.org/>.

New minimum requirements for 2024–2025 are highlighted in [Table 1: System Requirements for Online Testing](#) below.

Table 1: System Requirements for Online Testing

Category	Requirements
Devices	<p>Desktop: Windows, macOS</p> <p>Laptop: Windows, Chromebook®, macOS</p> <p>Tablets: iPad®, Windows</p>
Operating systems	<p>Windows 10: Versions 21H2 and 22H2</p> <p>Windows 11: Versions 21H2, 22H2, and 23H2</p> <p>Windows 10S, 11S, 11SE: Not supported</p> <p>ChromeOS: Release channel only; version 119 or later</p> <p>macOS: 13 and 14</p> <p>iOS: 16 and 17</p>
Processors	<p>Windows: Intel® compatible (32-bit or 64-bit)</p> <p>ChromeOS: Any</p> <p>macOS: Any</p> <p>iOS: Any</p>
Memory	<p>Windows: 2 GB (4 GB recommended)</p> <p>ChromeOS: 2 GB (4 GB recommended)</p> <p>macOS: 2 GB (4 GB recommended)</p> <p>iOS: 1 GB (2 GB recommended)</p>
Minimum screen size	9.5 inches for all devices
Minimum screen resolution	1024 x 768 for all devices Note: Most displays require no scaling. Windows sets the display scale to 100%.
Keyboard	Physical keyboard recommended for assessments with essays. Wired keyboard and mouse are strongly recommended.
Headphones	<p>Recommended for assessments with audio or for students with TTS accommodations.</p> <p>Sound Mode: Stereo Earpiece: Double Driver Unit Size: 32 mm</p> <p>Frequency Response: 20 – 20000 Hz</p> <p>Impedance: 32 ohms</p>

Acacia management and reporting system requirements

The management and reporting insights platform, known as Acacia, is supported on the latest versions of the following browsers:

- Google Chrome™
- Mozilla® Firefox®
- Mozilla Firefox LTS
- Microsoft® Edge™
- Safari®
- Safari on iPad®

The website is optimally viewed using a 1280 x 1024-pixel screen resolution. System functionality and screens may display, operate, or appear differently in different browsers and operating systems.

Part 4—Network requirements

Network connections

A stable, high-speed (wired or wireless) internet connection is required for online testing. The response time for each assessment depends on the reliability and speed of the school's internet connection.

Network settings

Network configuration settings should include all the elements noted below.

- Configure the content filters, firewalls, and proxy servers to allow traffic on the protocols and to the servers listed in [Network configurations](#) on page 12.
- Session timeouts on proxy servers and other devices should be set to at least 35 minutes. This will help limit interruptions during testing.
- Content caching must be disabled.
- If the client network uses any devices that perform traffic shaping, packet prioritization, or Quality of Service, the URLs specified in [URL allowlist](#) on page 12 must be used.
 - This guarantees the highest level of performance.
 - These URLs must be open or allowlisted.

If the internet connection is not working properly, students will need to complete their tests at a later time. All submitted test responses will be saved. When the student resumes testing, they will continue where they left off.

- Verify the network settings so the online testing applications will work properly.
- For any questions about network configurations, contact your network administrator or technology specialist.

Bandwidth

Bandwidth is the measure of the signaling capacity of a network. Bandwidth performance is affected on the internal local area network (LAN) traffic and internet traffic from the router. Regardless of hardware or network topology, the LAN should be analyzed to determine the potential for traffic bottlenecks. [Table 2: Testing Bandwidth by Number of Students Testing Concurrently](#) on the next page details the estimated average bandwidth used by the NWEA State Solutions Secure Browser.

Table 2: Testing Bandwidth by Number of Students Testing Concurrently

Number of students testing concurrently	Average estimated bandwidth used for testing
1	20 kbps
50	250–750 kbps (0.25–0.75 Mbps per second)
100	500–1500 kbps (0.5–1.5 Mbps)

Bandwidth varies during a student's testing experience. Some test pages contain low-bandwidth content, while others contain higher-bandwidth content, such as text-to-speech.

Consequently, the estimated average values in the column in [Table 2: Testing Bandwidth by Number of Students Testing Concurrently](#) above are based on computing averages from multiple tests and test subjects.

Note: When the NWEA State Solutions Secure Browser is first opened, bandwidth usage may be higher as it runs system, configuration, and network checks. The above guidelines apply after the browser has been opened.

Determining bandwidth requirements

To determine the necessary school bandwidth requirements, complete the following steps.

1. Run online readiness checks available at the [NWEA Online Readiness Tools website](#) to determine how many students can reasonably test concurrently. The bandwidth should not exceed the peak usage experienced when the test initially loads. Tests may include animations and interactive items, which may increase the bandwidth required. Refer to [Part 2—Online readiness tools](#) on page 4 for instructions.

Most school bandwidth levels are sufficient for wired networks. New switches generally operate at speeds of between 100 Mbps to 1000 Mbps. However, LAN performance can be hindered in cases where hubs are used instead of switches.

For internet networks, the most common bottleneck is the internet service provider's (ISP) router connection, which typically operates at speeds of between 5 Mbps to 100 Mbps.

2. Test and forecast whether your infrastructure has the capacity to accommodate needs:
 - a. Determine the average daily volume of internet traffic.
 - b. Determine the desired response time for non-test related applications that require internet connectivity and will operate during testing.
 - c. Determine the number of students who will test concurrently.

Size of test content

The size of the test is determined by two factors.

- The number of items on the test.
- The average size of each item.

The more items a test contains and the larger the average size item, the higher the bandwidth requirement.

NWEA State Solutions Secure Browser installation

The NWEA State Solutions Secure Browser is specifically designed for use in the test delivery platform. Local installation of the application on each individual testing workstation is recommended. This application can be installed on a network or a shared drive, and then testing workstations may run the application from this drive. The following performance impacts could occur under this configuration:

- There may be competition for network bandwidth, possibly slowing internet transmissions.
- The network or shared disk drive may also be subject to resource competition. Multiple clients reading from the network drive can reduce overall application performance.
- Due to the sensitivity of test-related data, encryption is always required. It is highly recommended that wireless traffic use WPA2/AES data encryption. Because encryption and decryption are part of the data exchange process, there may be a slight decrease in the overall network speed.

Wireless access points

It is recommended that each school maintain a ratio of wireless systems to wireless access points (WAPs) of no more than 20 to 1. Typically, test performance begins to deteriorate after this threshold is surpassed. In some instances, older WAPs have a lower capacity, which may lead to a slower rate and may cause performance degradation when more than 15 devices are concurrently attached.

Recommended workstations per wireless connection

The optimal (or maximum) number of student workstations (computers and tablets) supported by a single wireless connection depends on the type of networking standard used for the connection.

The two most common networking standards are 802.11g (54 Mbps) and the newer and faster standard, 802.11n (300 Mbps).

Both the access point, which emits the wireless signal, and the computer's wireless card, which receives the signal, will use one of these two standards.

The recommendations in [Table 3: Workstations Per Wireless Connection](#) on the next page are based on the standard in use.

Table 3: Workstations Per Wireless Connection

Wireless Card	802.11g Access Point	802.11n Access Point
802.11g wireless cards	20 workstations or devices	40 workstations or devices
802.11n wireless cards	20 workstations or devices	40 workstations or devices

Note: Refer to the manufacturer's WAP documentation for specific recommendations and guidelines.

Network diagnostic tools

NWEA provides [online readiness tools](#) to help determine a network's level of readiness for testing. It is available online at <https://securebrowser.state.nwea.org>. Refer to [System requirements check](#) on page 4 for more information.

If further diagnostic testing is needed, the following system-specific tools can help identify the network bottlenecks and problems.

Windows-specific tools

- **PRTG Traffic Grapher** (<http://www.paessler.com/prtg/>) is Windows software that monitors bandwidth usage and other network parameters via simple network management protocol (SNMP). It also contains a built-in packet sniffer. A freeware version is available.
- **PathPing** is a network utility included in the Windows operating system. It combines the functionality of Ping with a traceroute function (Windows filename: `tracert`). This provides details of the path between two hosts and Ping-like statistics for each node in the path based on samples taken over a time period.

macOS-specific tools

Use the **Network Utility** application, which is built in to macOS software.

Multi-platform tools

Wireshark (<http://www.wireshark.org/>) is a network protocol analyzer that has a large feature set and runs on most computing platforms including Windows, OS X, Linux, and UNIX.

TCPDump (<http://sourceforge.net/projects/tcpdump/>) is a common packet sniffer that runs under the command line and is compatible with most major operating systems (UNIX, Linux, and macOS). It allows the user to intercept and display data packets being transmitted or received over a network.

A Windows port called **WinDump** is also available (<http://www.winpcap.org/windump/>).

Ping, NSLookup, Netstat, and Traceroute (in Windows: `tracert`) is a set of standard UNIX network utilities. Versions of these utilities are included in all major operating systems (UNIX, Linux, Windows, and macOS).

Iperf (<http://sourceforge.net/projects/iperf/>) is a tool that measures maximum TCP bandwidth. This allows the user to tune various parameters and user datagram protocol (UDP) characteristics. Iperf reports bandwidth, delay jitter and datagram loss.

Network configurations

Protocols

All communication within the network takes place over the following internet port and protocol combinations. Ensure that the following ports are open for these systems.

Table 4: Ports and Protocols

Port and Protocol	Purpose
80 TCP	HTTP (initial connection only)
443 TCP	HTTPS (secure connection)

MIME types

Allow downloading and uploading of the following MIME types:

- Application/json
- Application/octet-stream
- Image/gif
- Image/png
- Image/svg+xml
- Multipart/form-data
- Printer/prn
- Text/html
- Text/xml
- Video/mp4

URL allowlist

Allow the following URLs for administration and testing to be accessed through the firewall:

- http://*.nwea.org
- https://*.nwea.org
- http://*.mapnwea.org
- https://*.mapnwea.org
- http://*.caltesting.org/
- https://*.caltesting.org/
- http://*.ets.org/
- https://*.ets.org/
- <http://hello.myfonts.net/>
- <https://hello.myfonts.net/>

Domain name resolutions (DNS)

All system URLs must be resolvable by the client hosts attempting to connect to the online testing system.

The client workstations must convert friendly names (URLs) to their corresponding IP address by requesting the information from the DNS server.

Email server

Make sure the following email addresses are allowlisted to ensure delivery.

- @nwea.org

Firewalls, content filters, and proxy servers

Note: For locations using SSL filtering, be aware that the SSL certificate for online testing uses san.ets.org as the CN (Common Name).

Configure firewalls, content filters, and proxy servers to allow traffic on the protocols listed above to the servers running the applications. Session timeouts on proxy servers and other devices should also be set to values greater than the average duration it takes a student to complete a given test.

QoS traffic shaping

If the client network uses any devices that perform traffic shaping, packet prioritization, or Quality of Service (QoS), then the URLs or IP addresses in [URL allowlist](#) on the previous page should be given a high level of priority. This ensures the greatest performance.

Virtualization guidelines

There are many different types of virtualization options for schools. Virtual environments can potentially impact both test security as well as the student testing experience. It is, therefore, the responsibility of district and school technology staff to ensure security and performance are maintained within virtualized environments. Compare and confirm security and performance in the virtualized environment. Performance comparisons should be completed by using the Online Readiness tools and taking tutorials and practice tests. The tools should first be used in a non-virtualized environment and then used in the virtualized environment to validate that security and performance is comparable. Virtualized environments, such as nComputing, VMWare, and Citrix XenDesktop have been used successfully.

Security

Test security is critical for high-stakes assessments. The student testing experience must be adequately controlled to prevent students from gaining access to information, communications, or other resources that could help them during the test. Additionally, test content and student responses must be secured across networks to protect against the potential exposure of test content. The NWEA State Solutions Secure Browser has significant security features that lock down the desktop to protect the integrity of the testing process.

Performance comparability

The system performance of the virtual environment must be comparable to a non-virtual environment. Verify that performance using the virtualized environment will not negatively impact the student's ability to test.

Critical security standards

Virtualization solutions should meet all of the following criteria for security standards:

- From login to submit, the desktop is secure, and the system does not allow access to any application, content, or other service beyond the NWEA State Solutions Secure Browser.
- From login to submit, the system does not allow any screen captures, printing, saving, or other electronic replication or duplication of the display screen or content of the test. This includes the viewing of test materials by district and school staff.

Critical performance standards

Ensure that virtualization solutions meet all of the following criteria to mimic a true testing environment:

- While logging in concurrently with the same number of clients that will be used during normal testing, no error messages are received.
- The first test item (question) of the practice test loads fully at the same speed as it does in a non-virtualized environment.
- While interacting with all practice test items, there are no noticeable lags or delays as compared to a non-virtualized environment.
- The text-to-speech (TTS) feature reads test questions aloud for the student. Be sure to use the tutorials and practice tests for verifying TTS functionality.
- When the practice test is submitted (completed normally), no error message is received, and the system responds at the same speed as compared to a non-virtualized environment.

Part 5—The NWEA State Solutions Secure Browser

About the NWEA State Solutions Secure Browser

All students must use the NWEA State Solutions Secure Browser to access the online assessments.

- The application prevents students from accessing other computer or internet applications or copying test information.
- Before any installation, check the administration rights to the computer or device.
- If you have disabled the auto-update feature on testing devices, confirm that all devices used for testing have the correct version of the NWEA State Solutions Secure Browser installed.

Note: The NWEA State Solutions Secure Browser is not the same as the NWEA Secure Testing Browser used for MAP Growth testing. If you also use MAP Growth, you do not need to uninstall that browser.

Windows installation and management

This section provides instructions for installing, managing, and uninstalling the Windows NWEA State Solutions Secure Browser on computers with supported Windows operating systems.

Note: All Windows installations require Read and Execute permissions to the program folder and Read and Write permissions to the user's home directory.

Important for 2024–2025: The NWEA State Solutions Secure Browser has been updated. The previous version must be uninstalled before installing the new version. Refer to [Uninstall the browser](#) on page 19 for instructions.

Download the installer

To download the installer:

1. Open a web browser and navigate to the [Online Readiness Tools](#) page.
2. Select the NWEA State Solutions Secure Browser MSI file to download and save the file.

Install the MSI package

Using an installation script

Note: This section only applies to system and network administrators with the appropriate privileges.

Network administrators can install the Windows NWEA State Solutions Secure Browser using an installation script executed by an administrator account on the machine. The script is designed to run without any human interaction (quiet switch).

You can use these scripts to install the NWEA State Solutions Secure Browser in the default directory (C:\Program Files for 32-bit, C:\Program Files (x86) for 64-bit) or any target directory of choice. Uninstallation can also be scripted.

Below are scripts for installation and uninstallation. Both require the script to have visibility to the MSI installation file and can only be executed by an administrator account on the machine. This is a Windows-based restriction, not a NWEA State Solutions Secure Browser restriction. The `msiexec` service that installs MSI files is used by administrators only.

Script conventions

<Source> = Complete path to the Secure Browser MSI installation file, including the MSI installation file name

Example: C:\MSI\NWEAStateSolutions.msi

<Target> = Complete path to the location where the application should be installed, if the default location (C:\Program Files) is not preferred.

Example: C:\MSI\Installation_Dir

Note: The target install directory does not have to be created in advance.

Installation script

```
msiexec /qb /i <Source> /quiet INSTALLDIR=<Target>  
STATEPARTNERCODE=ME
```

Example: `msiexec /qb /i C:\MSI\ NWEAStateSolutions.msi /quiet
INSTALLDIR=C:\MSI\Browser_Install STATEPARTNERCODE=ME`

Note: This configuration is only for the Maine Through Year Assessments. For other state assessments, contact your district or NWEA for the version of this guide for your state.

Uninstallation script

```
msiexec /x <Source> /quiet
```

Example: `msiexec /X C:\MSI\NWEAStateSolutions.msi /quiet`

Using mobile device management (MDM) software

The NWEA State Solutions Secure Browser may be installed and managed using third-party device management software. There are many options including Microsoft Intune.

The example steps below are for Microsoft Intune. If you use a different MDM software, refer to your support documentation or contact the MDM software's support team for further assistance if necessary.

1. In Intune, go to **Mobile Apps > Apps**.
2. Select **Add**.
3. In the **Select app type** area, select **Line-of-business** app, then choose **Select**.
4. Choose **Select app package file** to upload the MSI file.
5. The app details will be displayed. Select **OK** to add the app.
6. Select **App Information**.
7. In the **Command line arguments** field, enter the following: `/qb STATEPARTNERCODE=ME`

Note: This configuration is only for the Maine Through Year Assessments. For other state assessments, contact your district or NWEA for the version of this guide for your state.

8. Set the other information fields as desired.
9. Assign other settings as desired, then select **Create** to add the app to Intune.

Install via network

You can install the NWEA State Solutions Secure Browser to all computers on a network by copying browser files from the network to individual computers or through third-party programs to run the installers. This section describes how to install the application using a network. First, you should install the NWEA State Solutions Secure Browser to a shared drive, then install it from the network directory to the client computers.

1. Install the NWEA State Solutions Secure Browser onto the server:
 - a. Map the network directory to where the application was installed previously on each client machine.
 - b. In the network location where the application is installed, create a shortcut by right clicking the NWEA State Solutions Secure Browser icon and selecting **Create Shortcut**.

Optional: Rename the new shortcut. This becomes the shortcut link name used in step 4.
 - c. In the properties menu of the shortcut, change the path to use the mapped path as if on the client machine.

- d. Add the following command to each user (computer) profile, which will execute upon login through the user group login script:

```
COPY "<X> \ [ABC].lnk" "%USERPROFILE%\Desktop"
```

Note: <X> refers to the shared directory from which the application will be run. [ABC] refers the NWEA State Solutions Secure Browser file name. The script will need to reference the correct directory.

2. Copy the NWEA State Solutions Secure Browser from the network to the client computers:
- Identify the network directory where the NWEA State Solutions Secure Browser file was saved. These instructions will refer to that network directory as <X>.
 - Identify the target directory on the local user computers where the files will be copied.

Notes:

- These instructions will refer to that directory as <Y>.
 - User must have write access to <Y>.
 - Restricted users will have access only to certain folders on the local computers.
- Create a shortcut in the network directory by right clicking the NWEA State Solutions Secure Browser icon and selecting **Create Shortcut**.
 - Rename the new shortcut.
- Note:** In the shortcut properties, the **Target** and **Start In** attributes will show the <X> network installation directory.
- In both the **Target** and **Start In** attributes windows, change the shortcut properties to the <Y> directory instead of the default <X> network directory on the local computers.
- Note:** The NWEA State Solutions Secure Browser shortcut will point to the designated installation directory.
- Add the following lines to the login script for each user, replacing the actual local and source network directories for <Y> and <X>.

```
IF EXIST <Y> GOTO DONE  
XCOPY "<X>" "<Y>" /E /I  
COPY "<Y>\ [ABC].lnk" "%USERPROFILE%\Desktop"  
:DONE EXIT
```

Install manually

To install the NWEA State Solutions Secure Browser on Windows devices:

1. Launch the installer.
2. Follow the instructions in the installation wizard.
3. When prompted for the **Partner Code**, enter **ME** (not case-sensitive).

Note: This configuration is only for the Maine Through Year Assessments. For other state assessments, contact your district or NWEA for the version of this guide for your state.

4. Once the installation is complete, click **Finish**.
5. Launch the application by double-clicking the icon on the desktop or via the **Start** menu.

Uninstall the browser

To manually uninstall the NWEA State Solutions Secure Browser:

1. Right-click the **Start** button in the taskbar, open **Settings**, then select **Apps & Features**.
2. On the **Apps & Features** page, under **Apps & Features**, use the **Search this list** search box or scroll down to find the NWEA State Solutions Secure Browser.
3. Select the NWEA State Solutions Secure Browser, then select **Uninstall** to open the **Uninstall Wizard**.
4. Select **Next**, then **Yes**, then select **OK** to complete the uninstall process.

Disable Fast User Switching in Windows

Fast User Switching allows multiple users to be logged in concurrently. Disabling this function is strongly encouraged, as it allows a student to access multiple user accounts from a single computer.

Method 1: Group Policy editor

To disable Fast User Switching via Group Policy:

1. Right-click the **Start** button in the taskbar, then click **Run**.
2. In the **Search** text box, type `gpedit.msc` and select **OK**.
3. In the **Local Group Policy Editor** window, open **Administrative Templates** under **Local Computer Policy > Computer Configuration, System, and Logon**.
4. Select **Hide entry points for Fast User Switching**.
5. Select the **Edit policy setting** link in the left pane.
6. In the **Hide entry points for Fast User Switching** window, set **Hide entry points** to **Enabled**.

7. Select **OK** to save the setting and close the **Fast User Switching properties** window.
8. Close the **Local Group Policy Editor** window.

Method 2: Edit the registry

To disable Fast User Switching via the registry:

1. Right-click the **Start** button in the taskbar, then choose **Run**.
2. In the **Search** text box, type `regedit.exe` and select **OK**.
3. In the **Registry Editor** window, open **HKEY_LOCAL_MACHINE, SOFTWARE, Microsoft, Windows, CurrentVersion, Policies, and Open System**.
4. Right-click in the left pane of the **System** folder.
5. Select **DWORD (32-bit)** value under **New > Key**.
6. In the **New Value #1** text box, type `HideFastUserSwitching` and press **Enter**.
7. In the **Edit DWORD (32-bit) Value** window, Type `1` into the **Value data** text box and select **OK**.
8. Close the **Registry Editor** window.

Chromebook installation and management

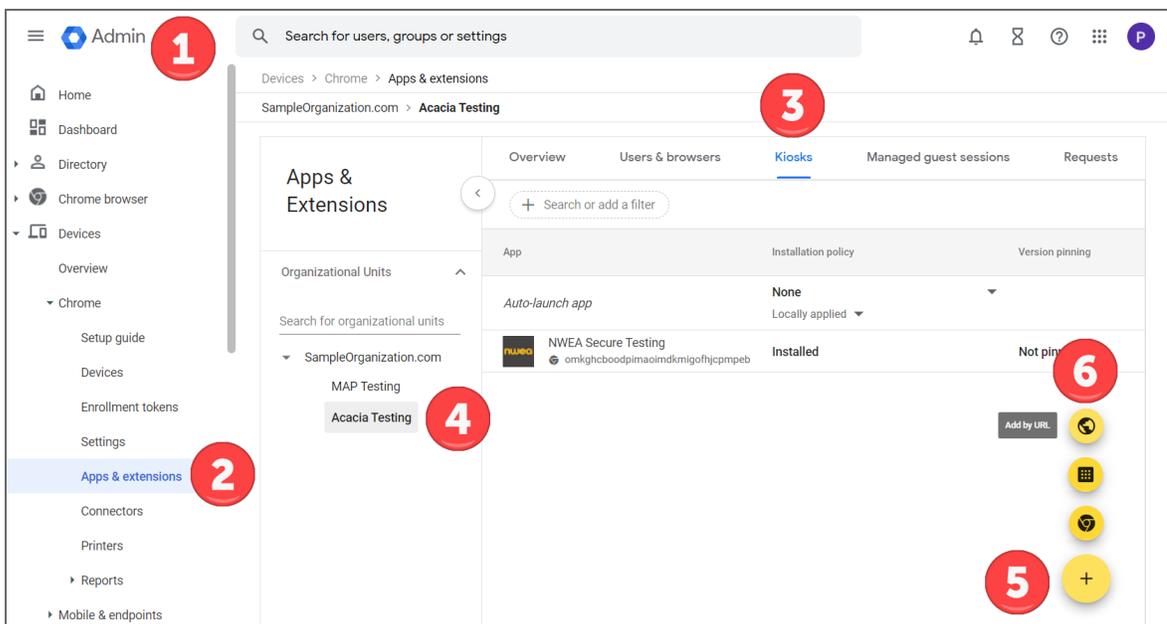
Important for 2024–2025: The Chrome testing app is being replaced by the Chrome Progressive Web App (PWA). Chrome apps will be deprecated soon. Refer to [Uninstall the legacy Chrome app](#) on page 23.

This guide walks you through how to install the NWEA State Solutions Secure Browser Chrome Progressive Web App (PWA), install and configure the required Chrome extension, and uninstall the legacy Chrome app. Chromebooks must be managed centrally through the Google admin console.

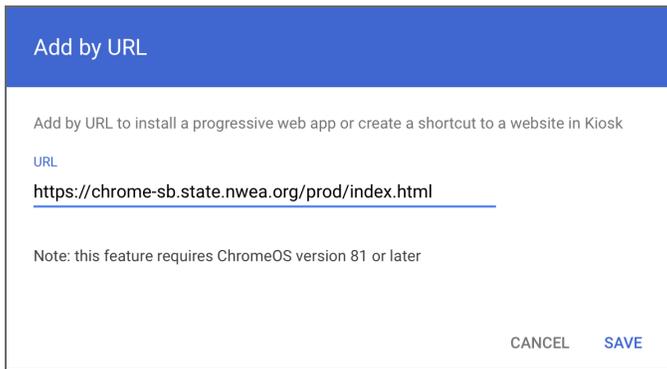
Install the PWA

To install the NWEA State Solutions Secure Browser PWA:

1. Open the Google Admin console.
2. In the navigation pane, select **Devices > Chrome > Apps & Extensions**.
3. In the **Apps & Extensions** pane, select the **Kiosks** tab.
4. In the **Organizational Units** list, select the organizational unit you want to install the PWA to.
5. In the bottom right, select the **+** button to see a list of options.
6. Select **Add by URL**.



7. In the **Add by URL** alert window, enter:
<https://chrome-sb.state.nwea.org/prod/index.html>
8. Select **Save**.

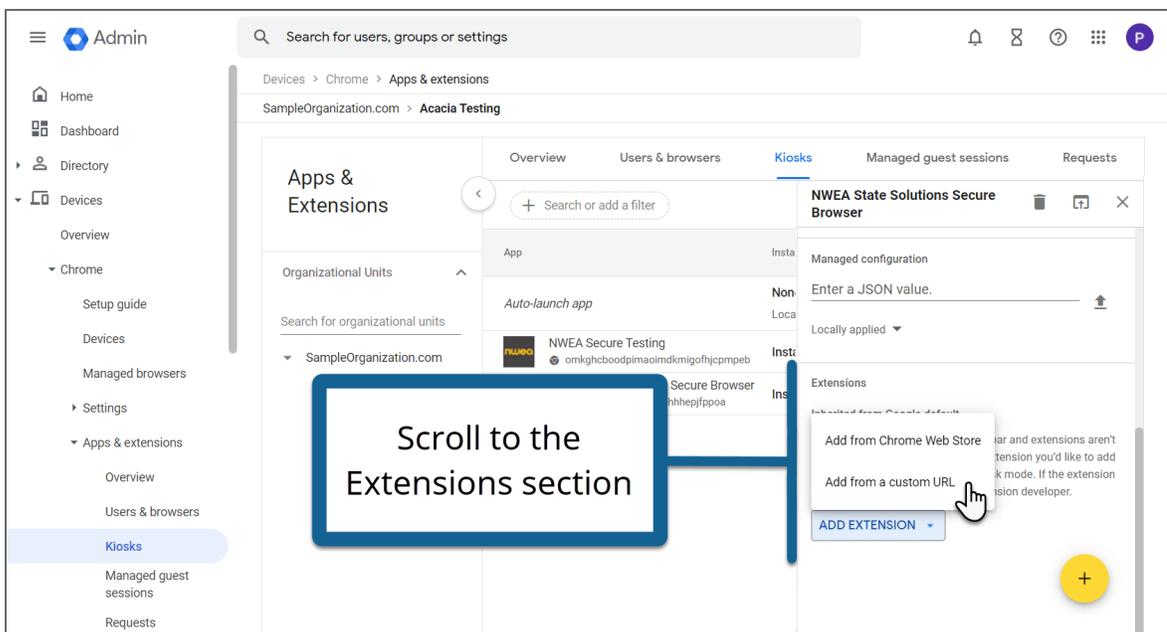


9. A permissions window appears. Select **Agree** to give the required permissions to the PWA.

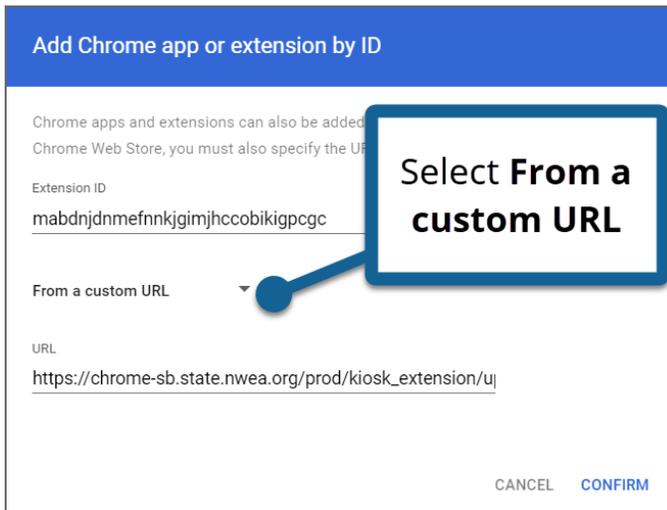
Configure the PWA and required extension

To configure the PWA and install the required extension:

1. The NWEA State Solutions Secure Browser app should appear in the list of installed apps, and a pane containing the configuration options for the app should appear. If the pane does not appear or you have closed it, select the app to open the pane.
2. In the **Extensions** section, select **Add Extension > Add from a custom URL**.



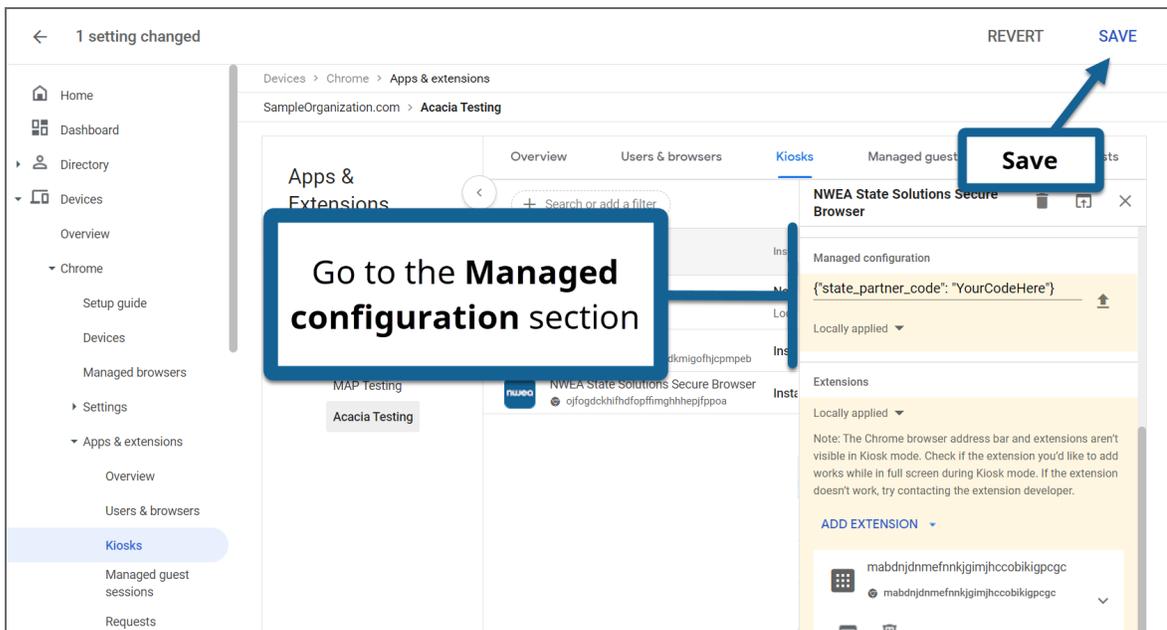
3. In the **Add Chrome app or extension by ID** alert window, open the menu and select **From a custom URL**.
4. Enter the following in the fields:
Extension ID: mabdnjdnme fnnkjgimjhccobikigpcgc
URL: https://chrome-sb.state.nwea.org/prod/kiosk_extension/updates.xml
5. Select **Confirm**.



6. In the **Managed Configuration** section, enter the following in the field labeled **Enter a JSON value**:

```
{"state_partner_code": "ME"}
```

7. Select **Save** in the upper right.



The PWA and its required extension are now installed and configured. The new NWEA State Solutions Secure Browser should appear in the list of kiosk apps on the Chromebook.

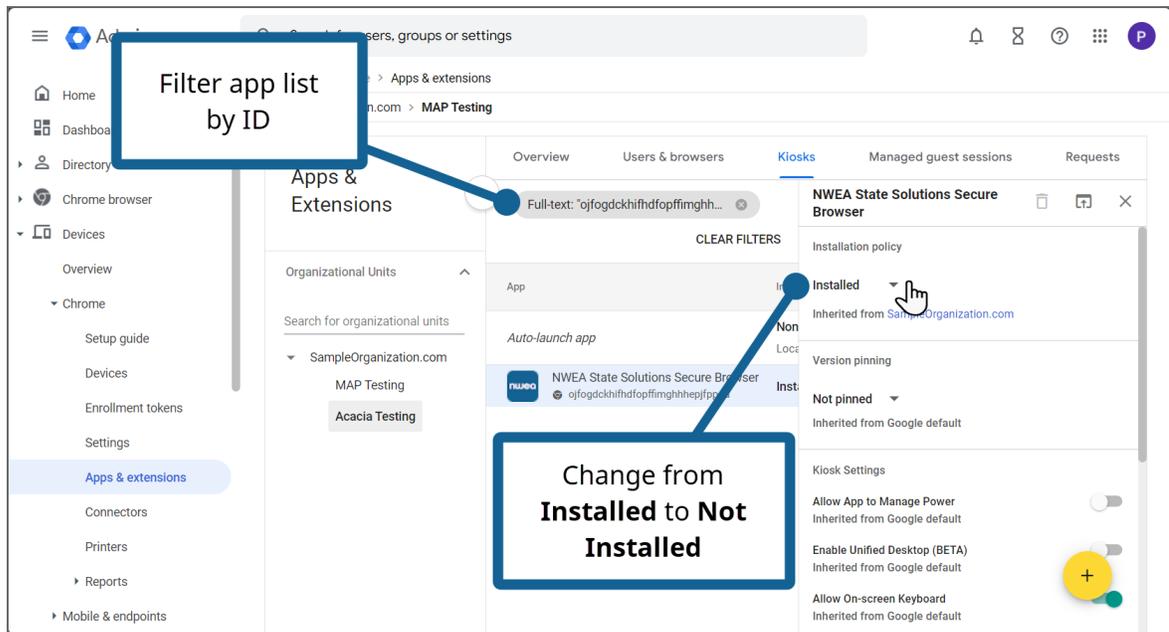
Uninstall the legacy Chrome app

To uninstall the legacy Chrome app:

1. Open the Google Admin console.
2. In the navigation pane, select **Devices > Chrome > Apps & Extensions**.
3. In the **Apps & Extensions** pane, select the **Kiosks** tab.

4. In the **Organizational Units** list, select the organizational unit for which the legacy app is installed.
5. In the search box above the list of apps, enter the following app ID:

```
ojfогdckhifhdfopffimghhhepjfppoa
```
6. The NWEA State Solutions Secure Browser app with this ID appears in the list of apps. Select the app.
7. In the pane on the right, under **Installation policy**, change the menu from **Installed** to **Not installed**.



8. Choose **Save** to save your changes. The legacy NWEA State Solutions Secure Browser app will no longer appear in the list of kiosk apps after a few minutes.

macOS installation and management

This section describes how to manage the NWEA State Solutions Secure Browser on supported macOS devices.

Important for 2024–2025: The NWEA State Solutions Secure Browser has been updated. Uninstall the previous version before installing the new version. Refer to [Uninstall the browser](#) on page 28 for instructions.

Device management software is preferred for deploying the NWEA State Solutions Secure Browser. Refer to [Using mobile device management \(MDM\) software](#) below.

Alternatively, districts can install the browser on each computer either manually or via Apple Remote Desktop. Refer to [Install manually](#) on page 27 and [Using Apple Remote Desktop \(ARD\)](#) on page 27.

macOS includes the native VoiceOver screen reader which students could attempt to use during testing. VoiceOver should be turned off during testing. If a student has VoiceOver enabled, refer to [Turn off VoiceOver](#) on page 29 for instructions for turning it off during testing. Visit [Accessibility Support at support.apple.com](#) for more information about managing accessibility features.

Download the installer

To download the installer:

1. Open a web browser and navigate to the [Online Readiness Tools](#) page.
2. Select the macOS NWEA State Solutions Secure Browser PKG file to download and save the installer.

Install the browser

Using mobile device management (MDM) software

The NWEA State Solutions Secure Browser may be installed and managed using third-party device management software. There are many options including **Simple MDM Server** at <https://simplemdm.com>, and **Jamf** at <https://www.jamf.com>.

Note: Deploying the NWEA State Solutions Secure Browser using device management software is required or preferred for later versions of macOS.

Use the app bundle identifier `org.nwea.NWEAStateSolutions`.

To deploy and configure the NWEA State Solutions Secure Browser:

- a. If you have not done so already, download the PKG installer. Refer to [Download the installer](#) above for instructions.

- b. Deploy the app to your devices. Links to instructions for some common MDM software are provided below. These third-party links may change without notice. Refer to the support documentation for the MDM software you use or contact the MDM software's support team for further assistance if necessary.
 - Simple MDM Server:
 - [Adding macOS Packages](#)
 - [Deploying and Updating Apps](#)
 - Jamf Pro: [Package Deployment for Jamf Pro](#)
- c. Add a configuration profile for the State Partner Code. **The example steps below are for Jamf Pro.** If you use a different MDM software, refer to your support documentation or contact the MDM software's support team for further assistance if necessary.
 - a. Log in to the Jamf Pro dashboard and select **Computers**.
 - b. Select **Configuration Profiles**, then choose **New**.
 - c. Go to **Options**, then **General Name**, and enter a display name.
 - d. Go to **Options**, then **Application & Custom Settings**.
 - e. Select **Upload**, then **Add**.
 - f. In the **Preference Domain** text box, enter `org.nwea.NWEAStateSolutions`
 - g. In the **PLIST** text box, enter the state partner code configuration as shown below:

```
<dict>
    <key>state_partner_code</key>
    <string>ME</string>
</dict>
```
 - h. Under **Scope**, select **Targets Computers**.
 - i. From the list of computers, select Add beside the ones on which you want this profile installed.
 - j. Select **Done**, then **Save**.
 - k. Verify that the profile is installed on a computer by looking in **System Preferences**. Select **Profiles**, then **Device Profiles**.
- d. Continue to [Upload the configuration profile \(MDM and ARD only\)](#) on page 28 to complete the installation.

Note: This configuration is only for the Maine Through Year Assessments. For other state assessments, contact your district or NWEA for the version of this guide for your state.

Using Apple Remote Desktop (ARD)

To install the NWEA State Solutions Secure Browser using ARD:

1. Log in to an administrator computer on the network. This computer should have **Apple Remote Desktop** installed and running.
2. If you have not done so already, download the installer.
3. Open **Apple Remote Desktop**.
4. In the **Apple Remote Desktop** window, select a **Computer List**.
5. Select the computers from the **Computer List** to install the NWEA State Solutions Secure Browser on.
6. Open **Manage**, then select **Copy Items**.
7. Select the PKG file you downloaded. Refer to [Download the installer](#) on page 25.
8. Select **Copy Options**, including the preferred destination on the target machine.
9. Select **Copy**.
10. Continue to [Upload the configuration profile \(MDM and ARD only\)](#) on the next page to complete the installation.

Install manually

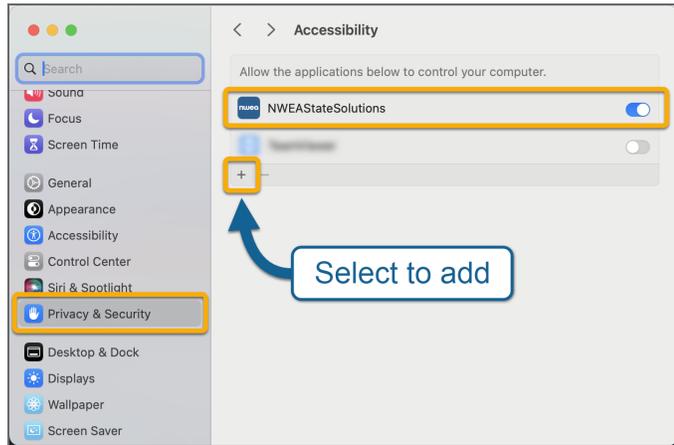
To install the NWEA State Solutions Secure Browser on a computer:

1. If you have not done so already, download the installer.
2. Open the PKG installer you downloaded to the computer.
3. Select **Continue** in the **Setup** window.
4. Specify where the application should be installed and click **Continue**.
5. Select **Install** in the confirmation window.
6. Enter the password and click **Install Software** in the pop-up window.
7. When prompted for the Partner Code, enter: ME (not case-sensitive).

Note: This configuration is only for the Maine Through Year Assessments. For other state assessments, contact your district or NWEA for the version of this guide for your state.

8. When the installation completes, click **Close** in the **Setup** window.
9. Select **Move to Trash** in the pop-up window to delete the installation file.
10. Add the app as a trusted application in the Security & Privacy settings:

- a. In **System Settings**, select **Privacy & Security**.
- b. In the list of privacy options, select **Accessibility**. A list of trusted applications appears.
- c. At the bottom of the list of trusted applications, select the **+** button and enter your password if prompted.
- d. Choose the NWEA State Solutions Secure Browser, then select **Open**.
- e. Confirm that the toggle for the NWEA State Solutions Secure Browser is on.



11. Launch the application by double-clicking the NWEA State Solutions Secure Browser in the appropriate folder.

Upload the configuration profile (MDM and ARD only)

If you are installing the NWEA State Solutions Secure Browser using mobile device management (MDM) software such as Jamf Pro, follow these additional steps to complete installation. Refer to the documentation for your MDM software for detailed instructions.

1. Download the MDM configuration profile from the [Online Readiness Tools](#) page.
2. In the MDM software, go to the configuration settings and select the option to upload a custom configuration profile.
3. Enter a profile name.
4. If prompted for an app bundle identifier, enter: `org.nwea.NWEASolutions`
5. Upload the MDM configuration profile.
6. Deploy the profile to the testing computers.

Uninstall the browser

The app can be uninstalled using MDM software or manually.

Using mobile device management

Links to instructions for some common MDM software are provided below. These third-party links may change without notice. Refer to the support documentation for the MDM software you use or contact the MDM software's support team for further assistance if necessary.

- **Jamf Pro:** [Uninstalling Packages](#)
- **Simple MDM Server:** [Deleting Apps](#)

Uninstall manually

If the NWEA State Solutions Secure Browser was installed manually, follow these steps to uninstall:

1. Open the **Applications** folder.
2. Right-click the NWEA State Solutions Secure Browser folder and select **Move to Trash**.
3. In **System Preferences**, select **Security & Privacy**.
4. In **Security and Privacy** settings, select the **Privacy** tab, then choose **Accessibility** in the list on the left.
5. Select the **Lock** icon in the bottom left to allow changes.
6. Select the NWEA State Solutions Secure Browser in the list of apps, then select the minus icon to remove it from the list.

Turn off VoiceOver

If students enable the screen reader VoiceOver, it can be turned off by using the keyboard shortcut **Command + F5**.

iOS installation and management

The Secure Browser application for iPad can be downloaded from the App store. The process for installing the application is the same as for any other iOS app.

For information about supported operating systems, hardware recommendations, and requirements for screen size, screen resolution, keyboards, and headphones, refer to [Requirements for Acacia testing online](#) on page 6.

The NWEA State Solutions Secure Browser for iOS automatically updates to the latest version. If auto-update is disabled, update via the App Store.

Install the app

Install manually

The NWEA State Solutions Secure Browser for online testing on iPads can be downloaded from the App store.

1. Open and search the Apple App Store for the NWEA State Solutions Secure Browser app.
2. Select the NWEA State Solutions Secure Browser app.
3. Tap the download icon to download and install the app.
4. Select **Update** if the window appears.
5. The app will download to the iPad home screen.
6. Launch the app. When prompted, enter the partner code: ME

Note: This configuration is only for the Maine Through Year Assessments. For other state assessments, contact your district or NWEA for the version of this guide for your state.

Using mobile device management (MDM) software

The NWEA State Solutions Secure Browser may be installed and managed using third-party device management software. There are many options including **Simple MDM Server** at <https://simplemdm.com>, and **Jamf** at <https://www.jamf.com>.

The example steps below are for Jamf Pro; if you use a different MDM software, refer to your support documentation or contact the MDM's support team for further assistance if necessary.

1. Log in to the Jamf Pro dashboard.
2. Select **Devices > Mobile Device Apps > New**.
3. Choose **App Store app** then select **Next**.
4. Search for the NWEA State Solutions Secure Browser.

5. In the search results, select **Add**. You should now see details about the app such as display name, version, etc.
6. Select **Scope > Targets > Add**.
7. Select the devices you want to add the app to.
8. Select **App Configuration**.
9. Add the following configuration dictionary:

```
<dict>
    <key>state_partner_code</key>
    <string>ME</string>
</dict>
```

Note: This configuration is only for the Maine Through Year Assessments. For other state assessments, contact your district or NWEA for the version of this guide for your state.

Uninstall the app

The example steps below are for Jamf Pro; if you use a different MDM software, refer to your support documentation or contact the MDM's support team for further assistance if necessary.

1. Log in to your Jamf Pro account.
2. Under the **Devices** tab, select **Mobile Device Apps**.
3. In the list of installed apps, select the NWEA State Solutions Secure Browser.
4. Select **Delete** in the bottom right corner.
5. In the confirmation window, select **Delete** again.

Assessment mode for iOS

The NWEA State Solutions Secure Browser uses Apple's Automatic Assessment Configuration (AAC) feature to implement assessment mode. Assessment mode prevents students from closing the app or navigating to other apps, and it automatically starts when the app is launched. After the student completes or logs out of the assessment and selects the option to exit the app, assessment mode ends. Refer to [Set up iPad and Mac to give tests and assessments](#) on the Apple support site for more information about assessment mode.

Follow these steps to launch the NWEA State Solutions Secure Browser app in assessment mode.

1. Open the app. During the system configuration check, a **Confirm App Self-Lock** notification pops up.
2. Select **Yes** to start assessment mode. Verify that the system check passes, and the app starts normally.
3. If you or a student selects **No**:
 - a. The Security Configuration portion of the system configuration check fails, giving error code 410: "This application runs only in single app mode. You must enable it in the 'Confirm App Self-Lock' pop-up notification."
 - b. Select the **Retry** button to run the system configuration check again and confirm app self-lock.

Close the NWEA State Solutions Secure Browser app

To close the NWEA State Solutions Secure Browser app:

1. After the student completes or logs out of their test, they are returned to the **Select a test to take** landing page. When they select **Exit** from this page, assessment mode ends.
2. Double-click the **Home** button or swipe up from the bottom of the screen, then pause in the center of the screen. This opens the App Switcher.
3. Locate the NWEA State Solutions Secure Browser app preview and slide it upward.

Updating the partner code

The partner code typically never changes, so organizations do not need to worry about changing the code regularly. However, if the partner code was entered incorrectly on a device, or if a school is instructed to update the partner code on a specific device, follow these instructions.

Mac or Windows

To update the partner code:

1. Open the NWEA State Solutions Secure Browser Preferences app.
 - Windows: Located in the **Start** menu > **NWEA State Solutions Secure Browser** folder
 - macOS: Located in **Applications** > **NWEA State Solutions Secure Browser** folder
2. Select **Network & Proxy**.
3. Update the **Partner Code** field. The code for Maine is **ME**.
4. Select **Save** to save your changes.

iOS

To update the partner code:

1. Open the **Settings** app.
2. Select the NWEA State Solutions Secure Browser.
3. Under the **State Partner** section, update the **Code** field. The code for Maine is **ME**.

Chromebook

To update the partner code:

1. Launch the NWEA State Solutions Secure Browser.
2. While the system checks are running, use the keyboard shortcut **Ctrl+Shift+5** to open the preferences window.

Note: Once the browser has fully launched, users cannot access the preferences window. Close the app and relaunch it to try again. Refer to [Chromebook installation and management](#) on page 21 for instructions.

3. Update the **State Partner Code** field. The code for Maine is **ME**.