Technical Specifications Manual for the Kaiapuni Assessment of Educational Outcomes (KĀʻEO)

For Technology Coordinators

2018-2019

Updated 1/14/19

Introduction to the Technical Specifications Manual

This manual provides information about the hardware, software and network configurations for running the operational and field tests of the 2018 Kaiapuni Assessment of Educational Outcomes (KĀʻEO). The System Requirements for Online Testing lists the minimum hardware and software requirements for online testing. Ensure your hardware complies with those requirements before undertaking the tasks described in this manual. If you have questions or concerns, please do not hesitate to contact the Help Desk at kaiapuni@hawaii.edu or 808-956-7834

Manual Content

- Section I, Network Configuration and Testing, provides information about configuring networks, and lists helpful networking diagnostic tools.
- Section II, Software Configuration, outlines configurations for operating systems.
- Appendix A, URLs Provided by KĀʻEO, lists KĀʻEO's URLs that should be whitelisted in your firewalls.
- Appendix B, Technology Coordinator Checklist, lists the activities required to prepare a facility for online testing.
- Appendix C, User Support
- Appendix D, Online System Requirements for KĀʻEO Testing

Intended Audience

This publication is intended for technology coordinators responsible for configuring the hardware, software, and network in a school's online testing environment. You should be familiar with the following concepts:

- Networking—Bandwidth, WiFi, routers, firewalls, whitelisting, and proxy servers.
- Configuring operating systems—Control Panel in Windows and System Preferences in macOS X.
- Configuring web browsers—Settings in Chrome, Firefox, and Internet Explorer.

Section I. Network Configuration and Testing

This section serves as a list of Internet connection and network infrastructure recommendations for schools administering the Kaiapuni Hawaiian Language Assessment exams. It consists of recommended best practices for a broad array of network configuration and diagnostic options to provide a smooth testing experience for both staff administering the exam and students taking the exam.

Network Configuration

This section provides guidance or requirements pertaining to networking configurations for online testing.

General Bandwidth Requirements

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 your school's Internet connection.

If the school's Internet connection is disconnected or loses service at any point before or during testing, students will need to complete their tests at a later time or on another day. Any answers they have already submitted will be saved, and students will resume their tests where they left off. (Students will return to the first unanswered item in the test.)

For the online testing applications to work properly, you may need to verify your network settings. If you are not sure whether your network is properly configured or you have questions, contact your school's network administrator or technology specialist or your Complex Area IT Manager (see table below). Complex Area Information Technology Managers are available to provide support to the school technology coordinators or designated technology point(s) of contact. You may also contact the Kaiapuni Help Desk at kaiapuni@hawaii.edu or 808-956-7834. See Appendix C for more information on the Help Desk.

IT Manager Complex Area

Ben Meyer	Section Head/Supervisor
Blain Shinno Farrington	Kaiser-Kalani
Stuart Yasui Kaimuki	McKinley-Roosevelt

Dean Yoshida Aiea	Moanalua-Radford
Kory Takemoto	Leilehua-Mililani-Waialua
Jon Kinoshita	Pearl City-Waipahu
Jordan Higa	Campbell-Kapolei
Ramon Cordero	Nanakuli-Waianae
Daijo Kaneshiro	Kailua-Kalaheo
Nicholas Alexander	Castle-Kahuku
Vacant	Hilo-Waiakea
Paul Sakamoto	Kau-Keaau-Pahoa
Jennifer Morgan	Honoka'a-Kealakehe-Kohala-Konawaena
Peter Ah Kee	Baldwin-Kekaulike-Maui
Ross Uedoi	Hana-Lahaina-Lana'i-Molokai
Byron Kapali	Kapaa-Kauai-Waimea

Guidance for Determining Required Bandwidth

A school's internet connection is the single point through which all data flows to and from the outside world. Any web pages, files, streaming video, and streaming audio must come through this connection to the school's computers. The amount of data that can be transferred over an internet connection is called "bandwidth", and is generally measured in Megabits per Second (Mbps). An Internet connection has both an Upload bandwidth and a Download bandwidth, which dictate how much total data can be sent out to the internet and how much can be received from the internet at any given time. More Download bandwidth is needed than Upload bandwidth.

Current recommendations from the State Educational Technology Directors Association[1] state that a school should have a minimum 1 Gbps down / 100 Mbps up of bandwidth per 1000 students and staff for its primary internet connection[2]. These bandwidth requirements should be taken seriously when looking at the school's primary internet connection, as more bandwidth is required to support a large number of devices, and especially important when accessing any

[1] http://setda.org/
[2] http://www.setda.org/wp-content/uploads/2013/09/SETDA_BroadbandImperative_May20Final.pdf

streaming video or audio portions of the exam. This also helps to handle spikes in network activity, such as when a large number of students are connecting during class time.

Bandwidth for Online Testing

In an online testing environment, the following factors contribute to determining the required bandwidth:

- Number of Students Simultaneously Testing—As the number of students testing at one time increases, the required bandwidth also increases.
- Size of the Test Content—The size of a test's content is determined by two factors: (1) the number of items on the test and (2) the average size of each item. The more items a test contains and the larger the average test item, the higher the bandwidth requirement for a given test. For example, some writing tests have a few questions to which the student composes a response, and these tests are small. In contrast, some science tests have animations or simulations; these tests are large.
- Hubs or Switches—LAN performance can be hindered when hubs are used instead of switches. A hub broadcasts signals from various network devices to propagate across the network, potentially saturating the network and causing traffic competition or data collisions. If you use hubs, ensure they have enough bandwidth to handle the propagation.
- ISP Router—For Internet networks, the most common bottleneck is the ISP's router connection, which typically operates at speeds of between 1.5M bits per second and 100M bits per second. Network administrators should spend time prior to test administration determining if their Internet infrastructure has the capacity to accommodate online testing at the required performance level.
- Encryption—Encryption at WAPs may contribute to bandwidth usage. If you use encryption, ensure the WAPs have enough bandwidth to prevent degradation of performance.
- Required Response Time—When a network's bandwidth cannot service the amount of data requested by clients, latency starts to accumulate and the students experience delays. Ensure your network's bandwidth is high enough to support the required response times between the browsers and the servers.

Table 1 displays the estimated average bandwidth used by the secure browser for testing. When designing your network for online testing, ensure that the available bandwidth can support these values.

Table 1. Average Bandwidth Used by Secure Browser for Testing

Number of Students Testing Concurrently in School or Building	Average Estimated Bandwidth Consumed During Testing
1	5-15K bits/sec
50	250-750K bits/sec
100	500-1500K bits/sec

Required Ports and Protocols

Table 2 lists the ports and protocols used by the Test Delivery System. Ensure that all content filters, firewalls, and proxy servers are open accordingly.

Table 2. Ports and Protocols for Test Delivery System

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

Whitelisting Test Site URLs

If the school's filtering system has both internal and external filtering, the URLs for the testing sites (See URLs for Testing Sites) must be whitelisted in both filters. Please see your vendor's documentation for specific instructions. Also, be sure to whitelist these URLs in any multilayer filtering system (such as local and global layers).

Configuration for Domain Name Resolution

Appendix A lists URLs required for KĀ‘EO testing. Ensure the testing machines have access to a server that can resolve those names.

Configuring Session Timeouts

Session timeouts on proxy servers and other devices should be set to values greater than the average time it takes a student to participate in a test session or to complete a given test. For example, if your school determines that students will test in 60-minute sessions, then consider setting the session timeout to 65 or 70 minutes.

Data Caching

Data caching is a technique by which an intermediate server checks if it can serve the client's requests instead of a downstream server. While data caching is a good strategy in some situations, its overhead is detrimental in the online testing environment. Ensure all intermediate network elements, such as proxy servers, do not cache data.

Configuring Quality of Service and Traffic Shaping

If your testing network includes devices that perform traffic shaping, packet prioritization, or Quality of Service (QoS), ensure the URLs in Appendix A have high priority.

Configuring Network Settings for Online Testing

Local Area Network (LAN) settings on testing machines should be set to allow access to the local network and to the test URLs as listed in Appendix A: URLs for Testing Site.

Uninterruptible Power Supply

Any equipment providing the internet connection such as modems, routers, firewalls, servers, switches, or other involved systems should be connected to an Uninterruptible Power Supply or UPS[3] system in the event of a power outage. This will also protect equipment from power surges or other electrical issues which could result in a longer outage due equipment failure. Please check to make sure that the UPS unit is rated to handle the power requirements of the equipment drawing power from it[4].

Network Diagnostic Tools

You should do a performance analysis of your networking infrastructure to identify any bottlenecks that may impact test performance. The choice of diagnostic tool depends on the operating system running the tool, the network administrator's technical knowledge, and the desired level of network analysis. A number of network diagnostic tools are available, as described in the following sections.

Windows-Specific Tools

- **PRTG Traffic Grapher** (www.paessler.com/prtg) 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.

[3] https://en.wikipedia.org/wiki/Uninterruptible_power_supply
[4] http://www.apc.com/us/en/tools/ups_selector/

- **NTttcp** (www.microsoft.com/whdc/device/network/TCP_tool.mspx) is a multithreaded, asynchronous application that sends and receives data between two or more endpoints and reports the network performance for the duration of the transfer.
- **Pathping** is a network utility included in Windows. It combines the functionality of the ping and tracert commands by providing 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.

OS X-Specific Tools

- **Network Utility.app** is built into mac OS X.

Multi-Platform Tools

- **Wireshark** (www.wireshark.org) is a network protocol analyzer. It has a large feature set and runs on most platforms including Windows, OS X, and Linux.
- **TCPDump** (http://sourceforge.net/projects/tcpdump) is a common packet sniffer that runs from the command line on Linux and OS X. It can intercept and display data packets being transmitted or received over a network. A Windows version WinDump is available (www.winpcap.org/windump/).
- **Ping, NSLookup, Netstat, Traceroute** is a set of standard UNIX network utilities. Versions of these utilities are included in Linux, Windows, and OS X, but may not be installed by default.
- **Iperf** (http://sourceforge.net/projects/iperf/) measures maximum TCP bandwidth, allowing the tuning of various parameters and User Datagram Protocol (UDP) characteristics. Iperf reports bandwidth, delay jitter, and datagram loss.

Section II. Hardware Configuration

This section provides topology guidance for printers and WAPs.

Connections between Printers and Computers

Test Administrators can print test codes and paper versions of the exams (for students with the print-on-request accommodation). Nevertheless, to maintain a secure test environment, the Test Administrator's computer should be connected to a single local or network printer in the testing room, and only the Test Administrator's computer should have access to that printer.

Wireless Networking and Determining the Number of Wireless Access Points

Wireless networking standards have evolved over the years, with the following being the most commonly deployed:

- 802.11ac has a theoretical throughput of up to 1G bits per second.
- 802.11n has a throughput of up to 300M bits per second.
- 802.11g has a theoretical throughput of up to 54M bits per second.
- 802.11b has a theoretical throughput of 11M bits per second.

The recommended number of devices supported by a single wireless connection depends on the standard used for the connection. The two most common networking standards are 802.11g (54Mbps) and 802.11n (300Mbps). Table 3 lists recommendations for network topology in which the WAP provides 802.11g and the testing devices provide 802.11g, 802.11n, or a mixture of the two. Refer to your WAP documentation for specific recommendations and guidelines for these or other standards.

Table 3. Recommended Ratios of Devices to Wireless Access Points

Testing Device	Ratio of Devices to 802.11g WAP	Ratio of Devices to 802.11n WAP
802.11g	20	40
802.11n	20	40
Mix of 802.11g and 802.11n	20	40–50 (depending on the mix of wireless cards used)

Regardless of the number of WAPs, each should be configured to use WPA2/AES data encryption.

Network Security

When possible, separate networks should be maintained for student access and for faculty/staff access. This is to prevent unauthorized access by students to sensitive materials such as private student information, grades, and so forth. In addition, access to either network should be restricted to school-owned devices only to prevent compromise by hacking, virus, or other issues brought by personally owned laptops or systems.

A third option is to provide a “guest” network for these devices that is separate from the student and faculty/staff networks, but this is done at a higher cost and maintenance to the school. Schools should try to balance the need for non-school device access and the security of their network.

Network access for all devices should require a login username and password to authorize access. WiFi may be further secured by using WPA2 for encryption of wireless communication.

All faculty and staff should sign a notice stating their understanding of the handling of private student information. The above plus students should sign an Acceptable Use Policy which dictates what uses of the network are allowed and which are not (academic use, no hacking, no unauthorized access to private information). Notices should be kept with the applicable faculty/staff or student’s file with the school.

Section III. Software Configuration

This section describes how to configure the operating systems and web browsers for online testing.

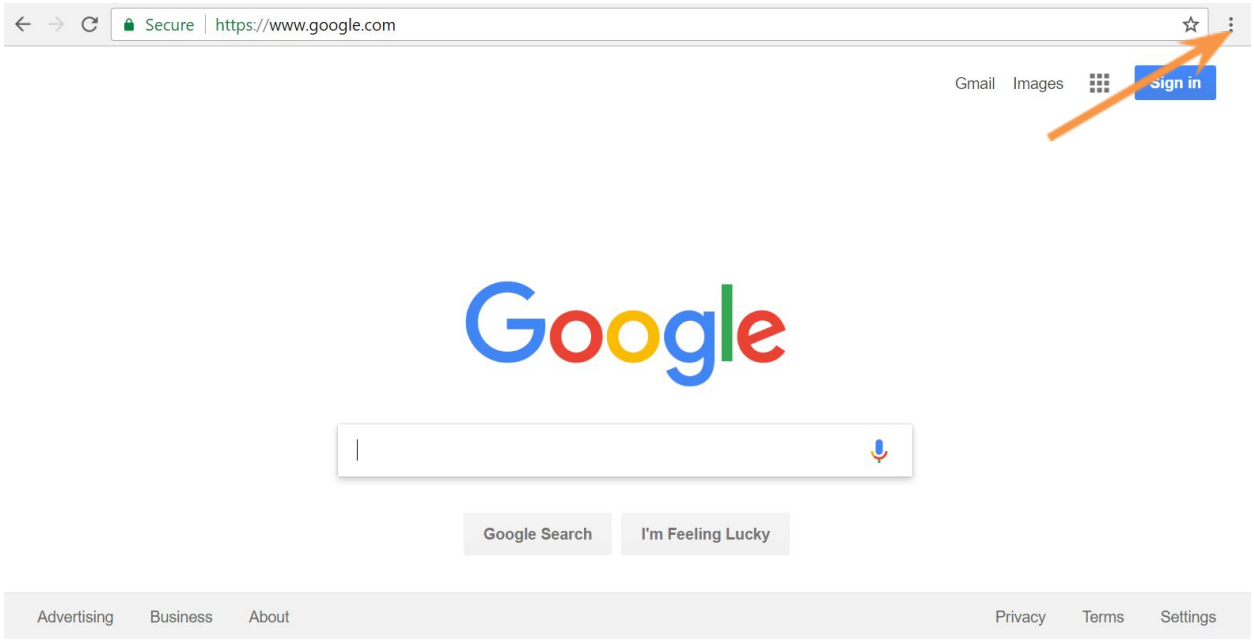
Configuring Commercially Available Browsers

Before testing can begin each computer must have an approved browser installed that is properly configured for testing. The latest patched versions of Chrome, Firefox, or Internet Explorer can be safely used for testing on all recent operating systems. For a detailed list of all supported browsers and versions across operating systems, please see Appendix D: Online System Requirements for the KĀ‘EO assessments.

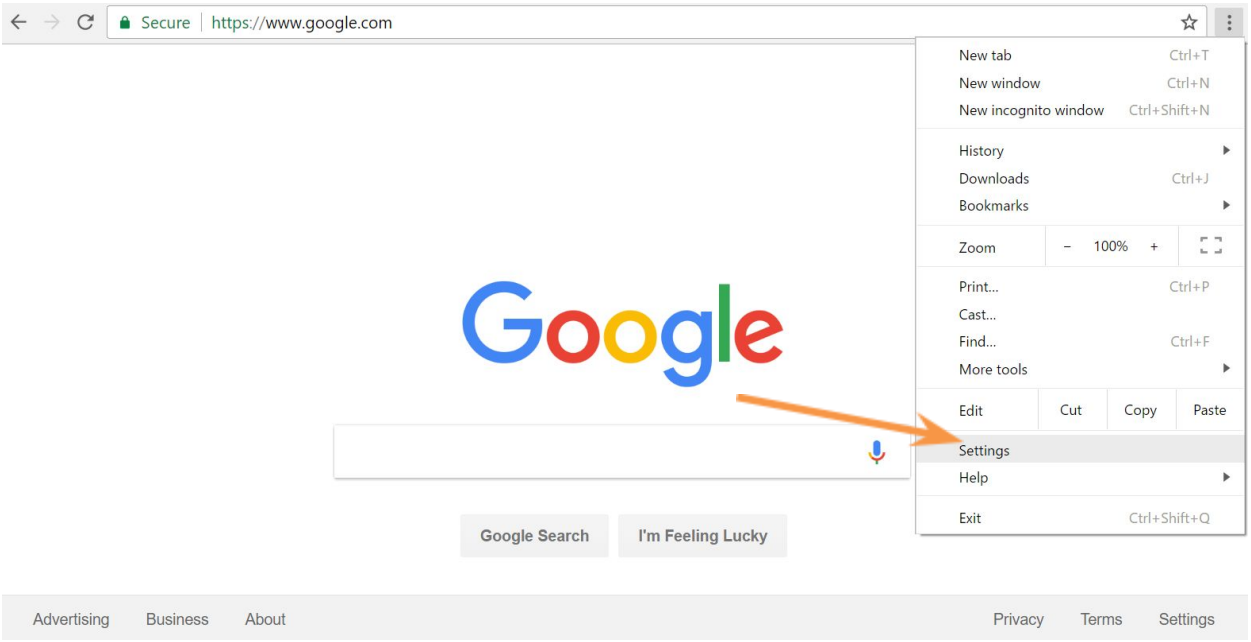
The following browser settings should be checked to ensure test security throughout the testing window: (1) Disable Auto-fill / Auto-complete, (2) Disable Passcodes Save, (3) Enable Clearing of Cookies/Cache on Close, and (4) Turn off page translation (Google only).

Chrome (v56)

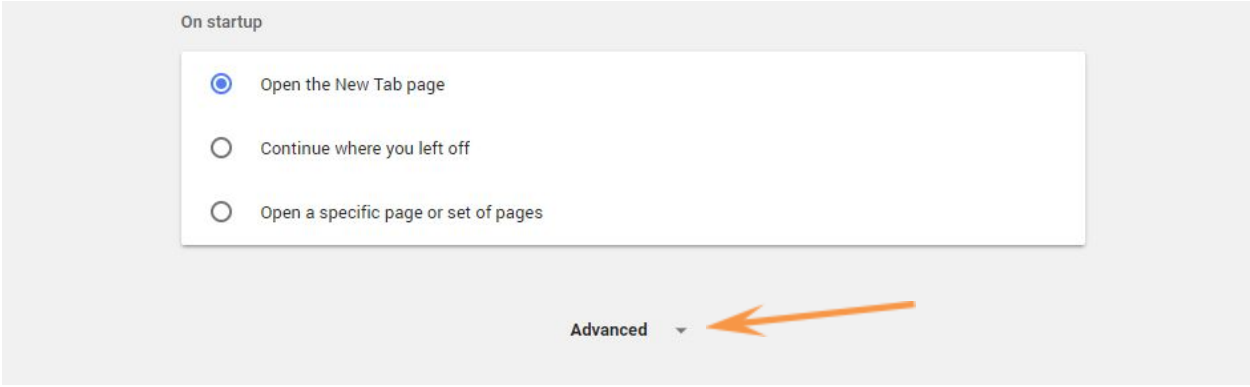
Step 1 – Open Chrome and locate the menu



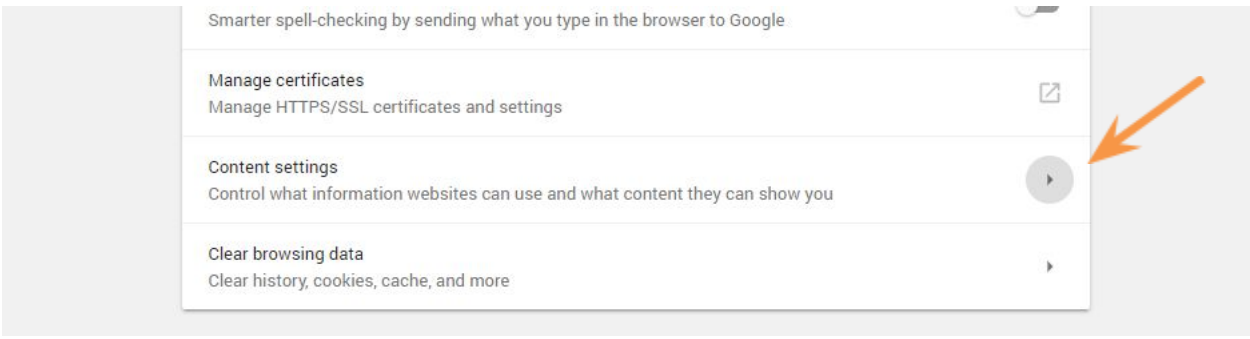
Step 2 – Open Chrome’s settings



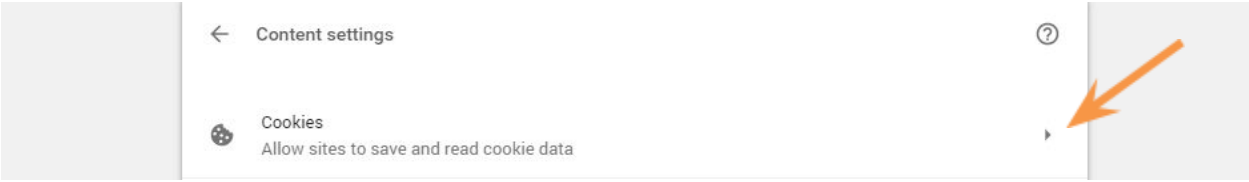
Step 3 – Select ‘Advanced Settings’



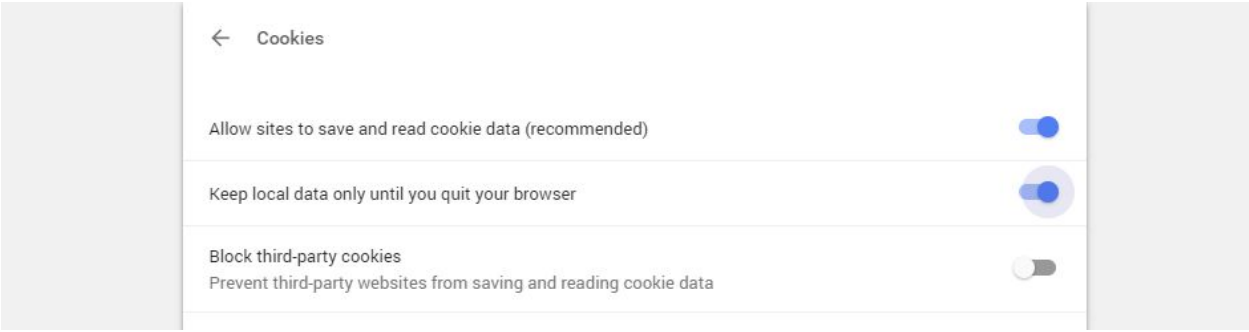
Step 4 – Scroll down and select ‘Content Settings’ by click the button on the right side



Step 5 – Next, select the ‘Cookies’ menu

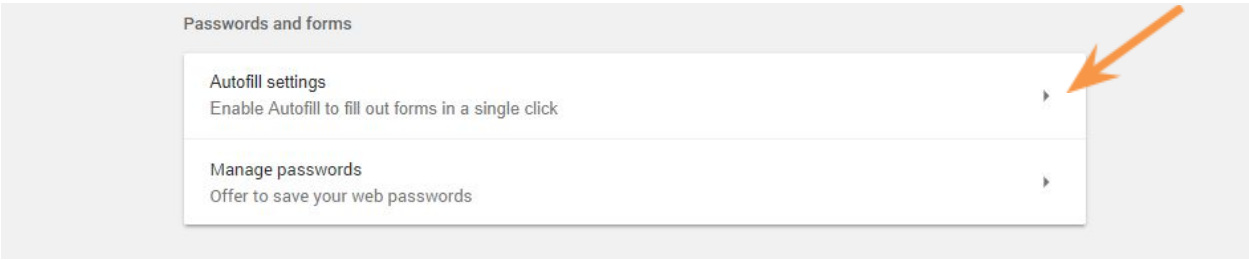


Step 6 – Turn on ‘Keep local data only until you quit your browser’ then exit the ‘Cookies’ menu



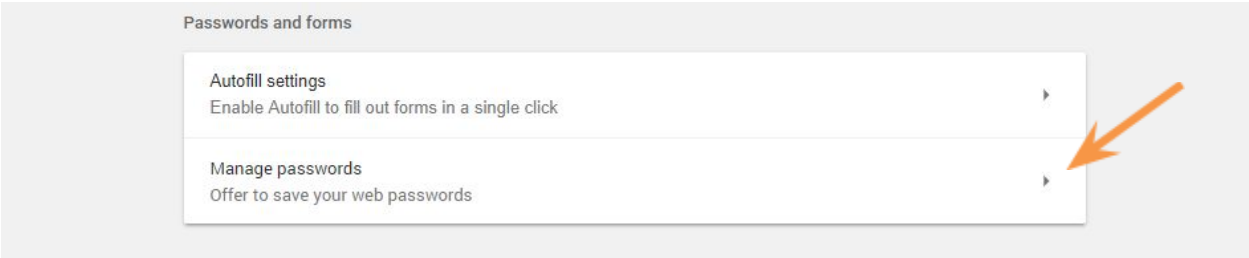
Step 7 – Exit the ‘Content’ menu

Step 8 – Scroll down to the passwords and forms section and select ‘Autofill settings’

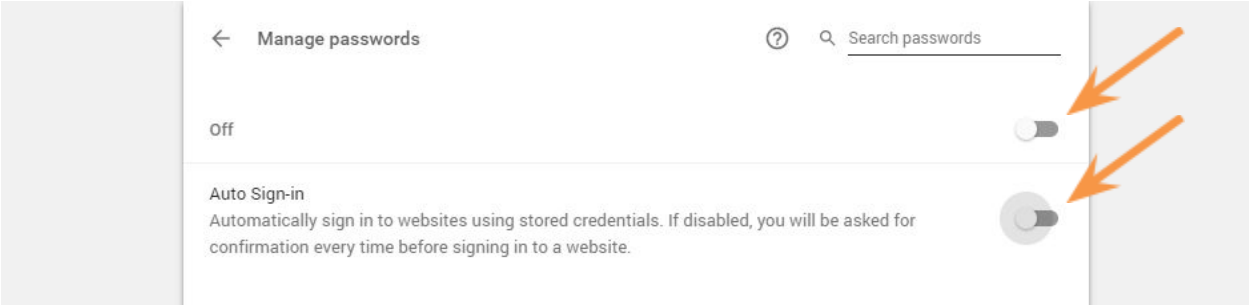


Step 9 – Turn off autofill and exit the auto fill menu

Step 10 – Select ‘Manage passwords’

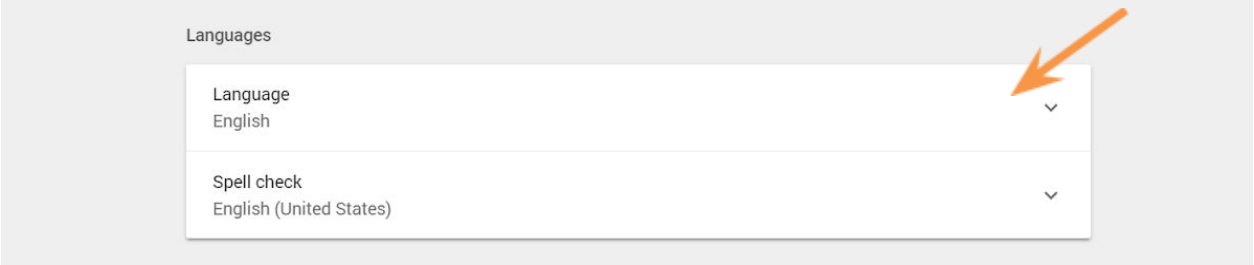


Step 11 – Turn off password management and ‘Auto Sign-in’

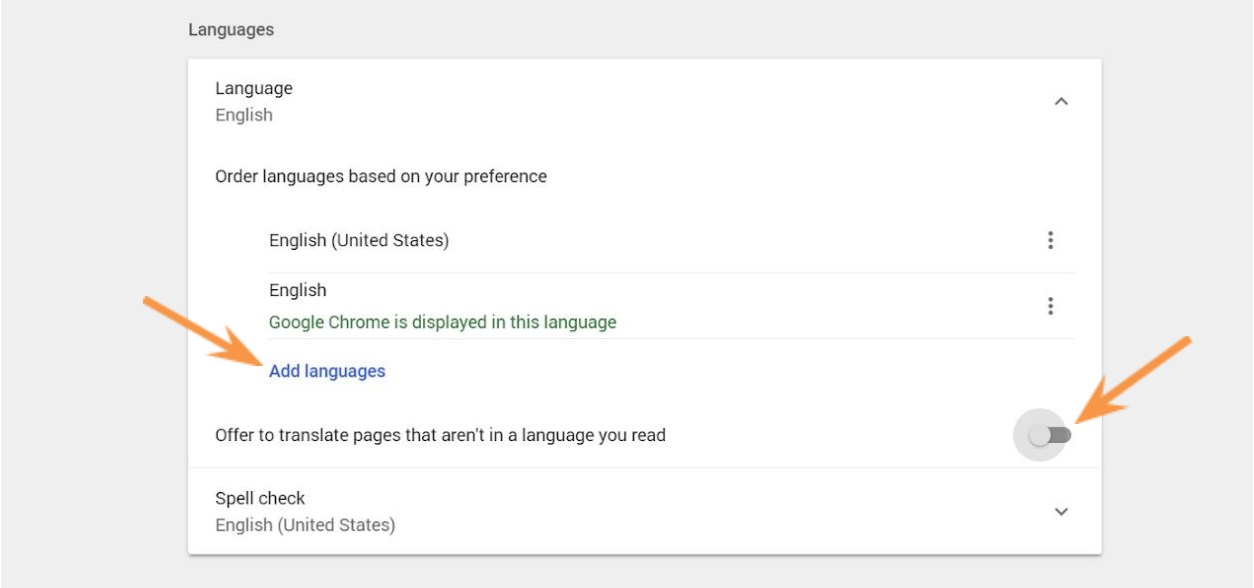


Step 12 - Exit passwords

Step 13 - Open the languages menu



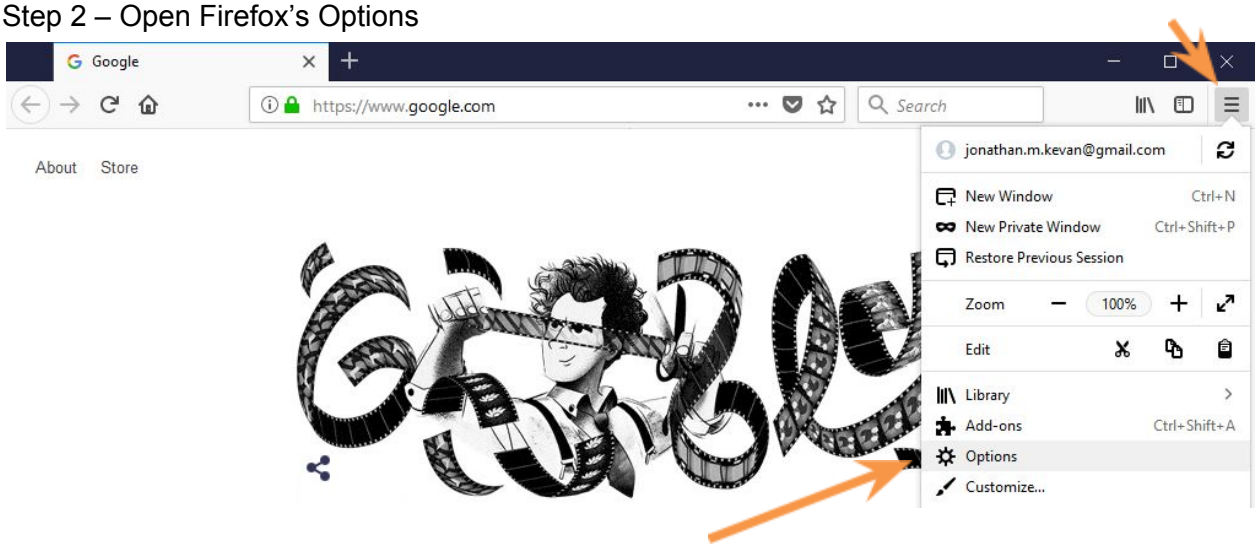
Step 14 - Either turn off ‘Offer to translate pages that aren’t in a language you read’ or select ‘Add languages’ and include Hawaiian as preferred languages.



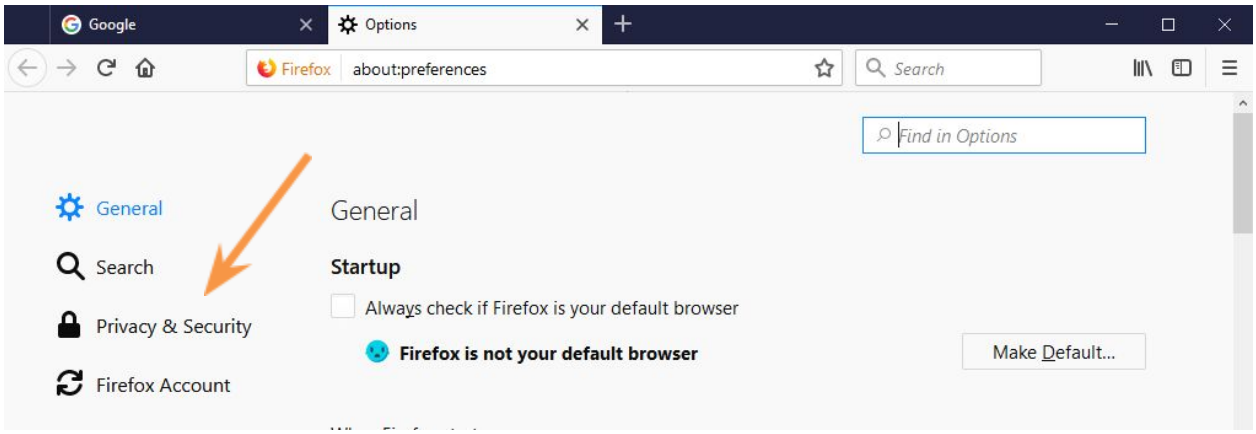
Firefox (v57)

Step 1 – Open Firefox and locate the menu

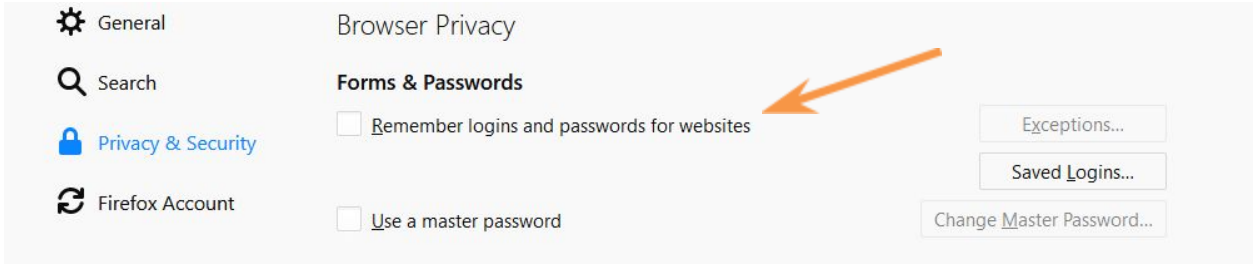
Step 2 – Open Firefox's Options



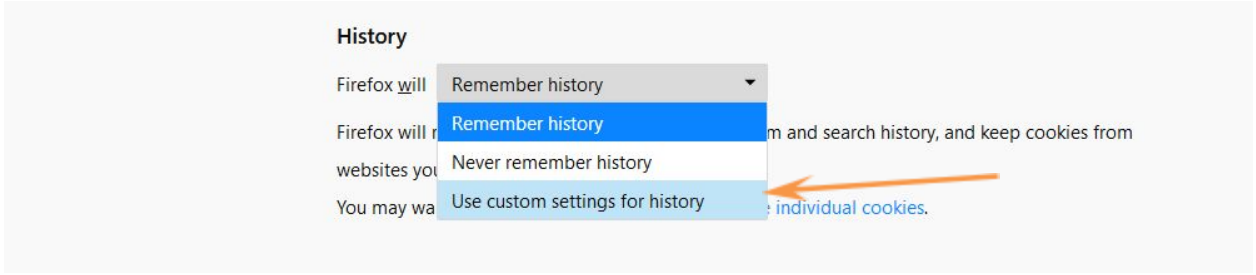
Step 3 – Select ‘Privacy & Security’



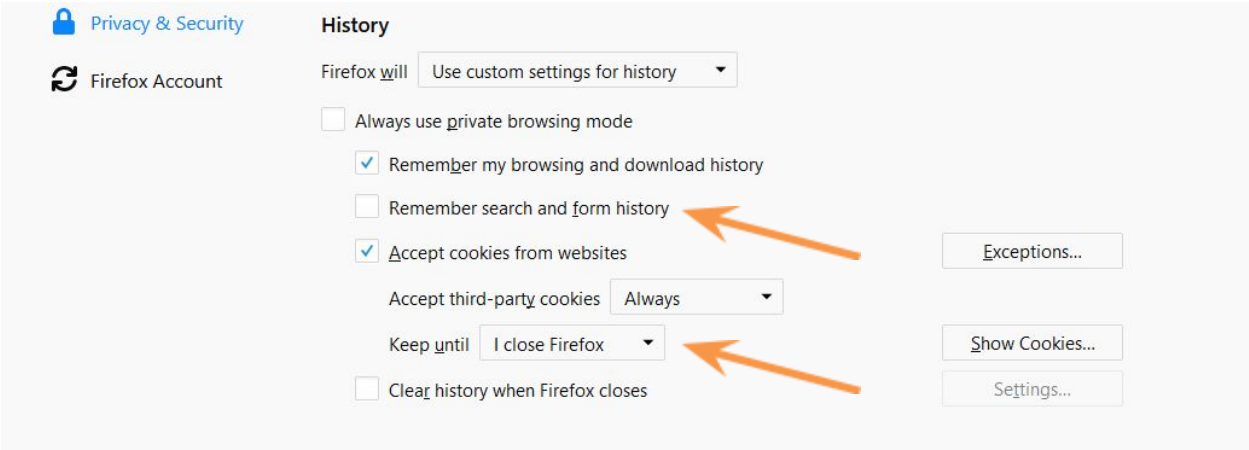
Step 4 – Deselect ‘Remember logins and passwords for websites’



Step 5 – Just below select ‘Use custom settings for history’

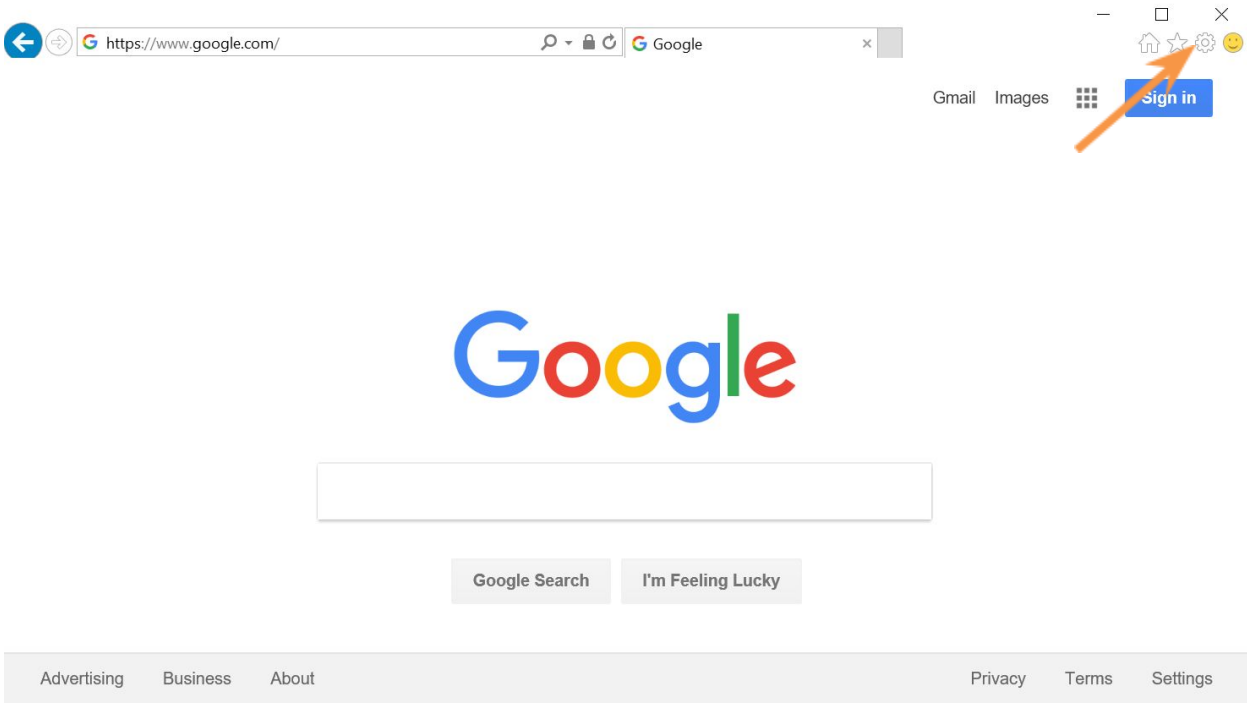


Step 6 – Deselect ‘Remember search and form history’ & set ‘Keep until:’ to ‘I close Firefox’

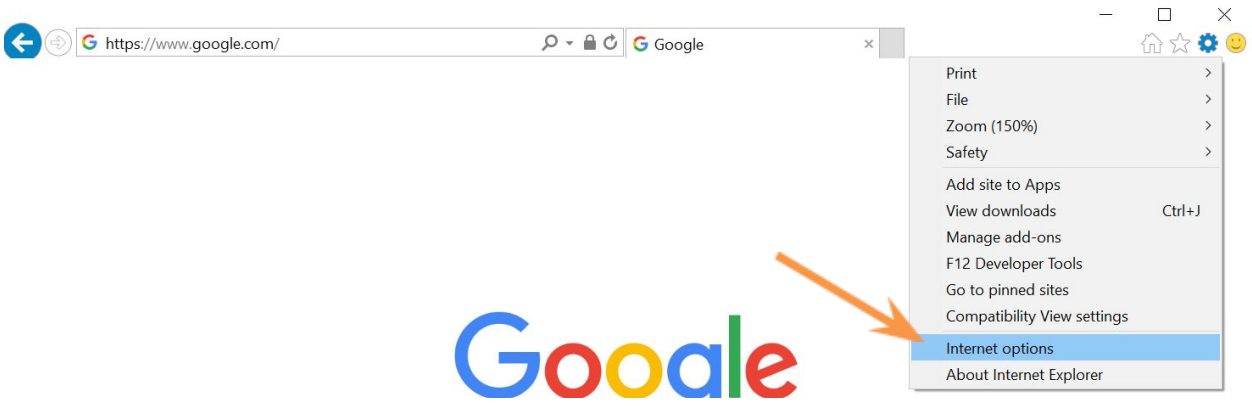


Internet Explorer (v11)

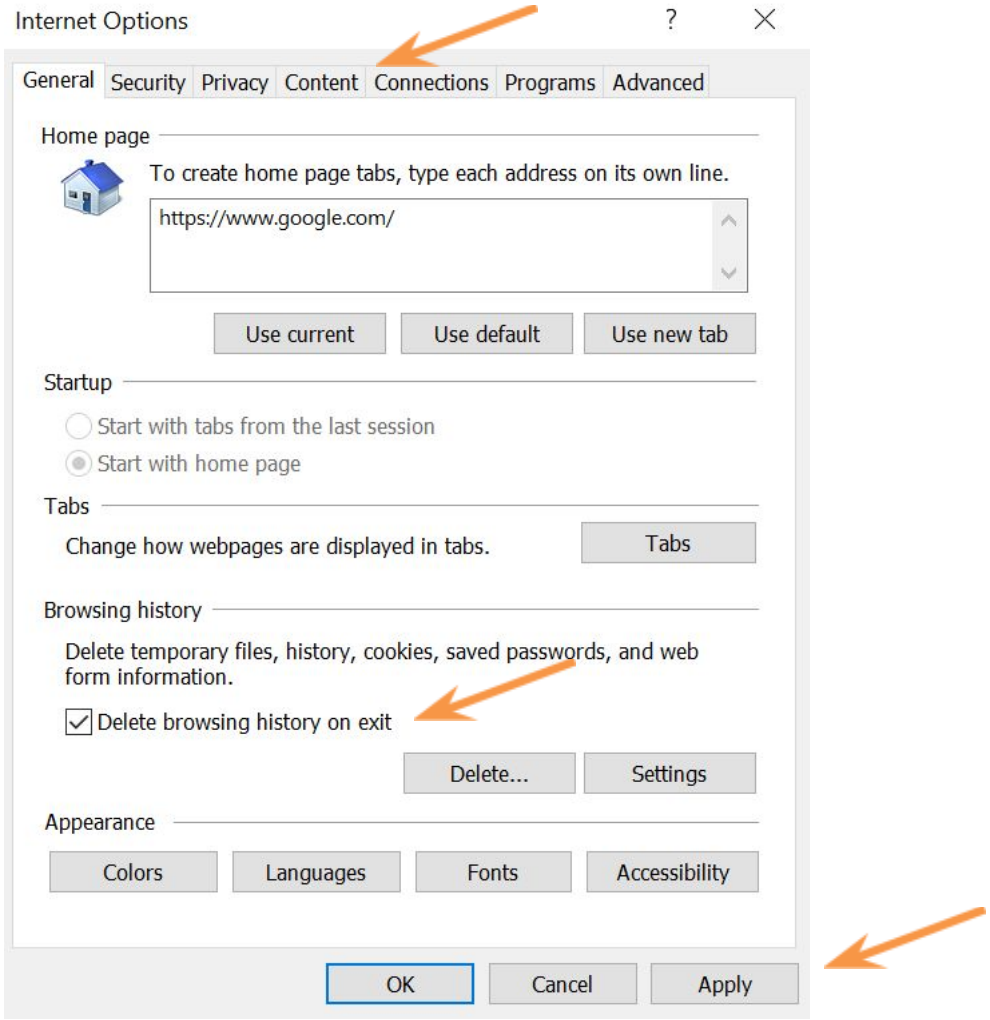
Step 1 – Open Internet Explorer and locate the menu



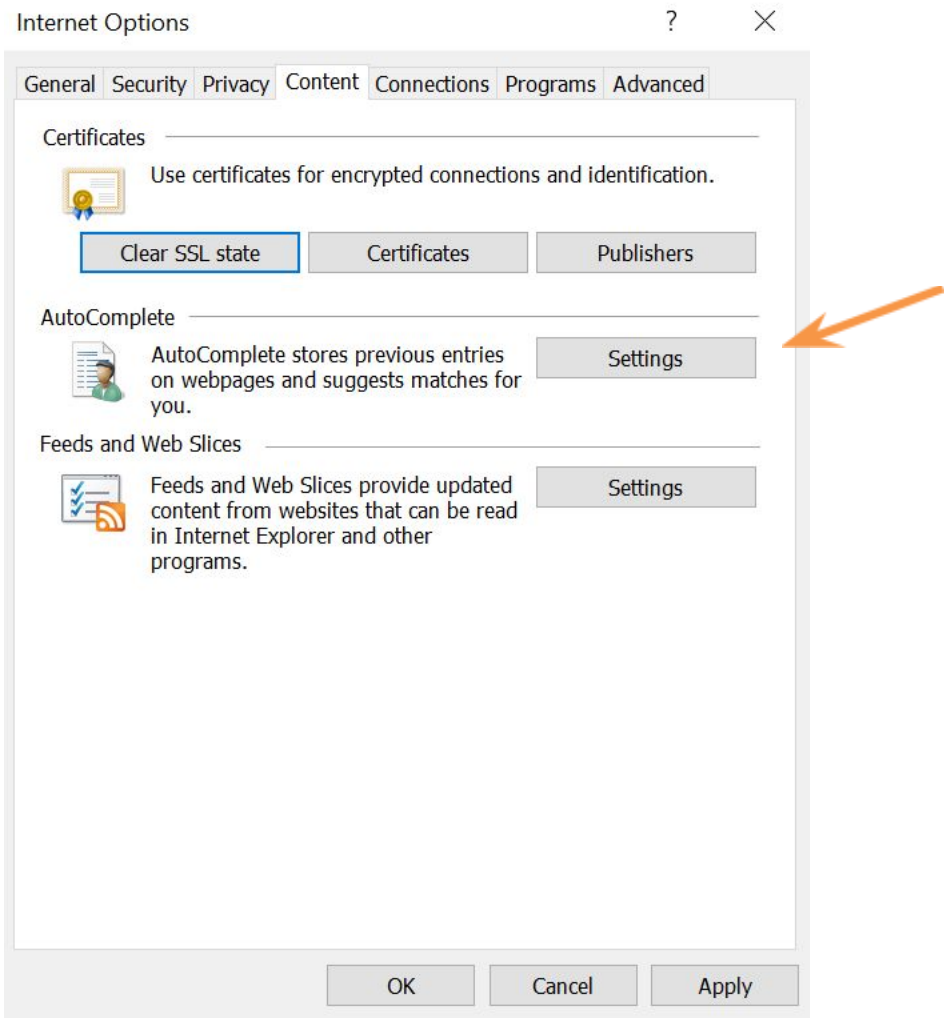
Step 2 – Select ‘Internet options’



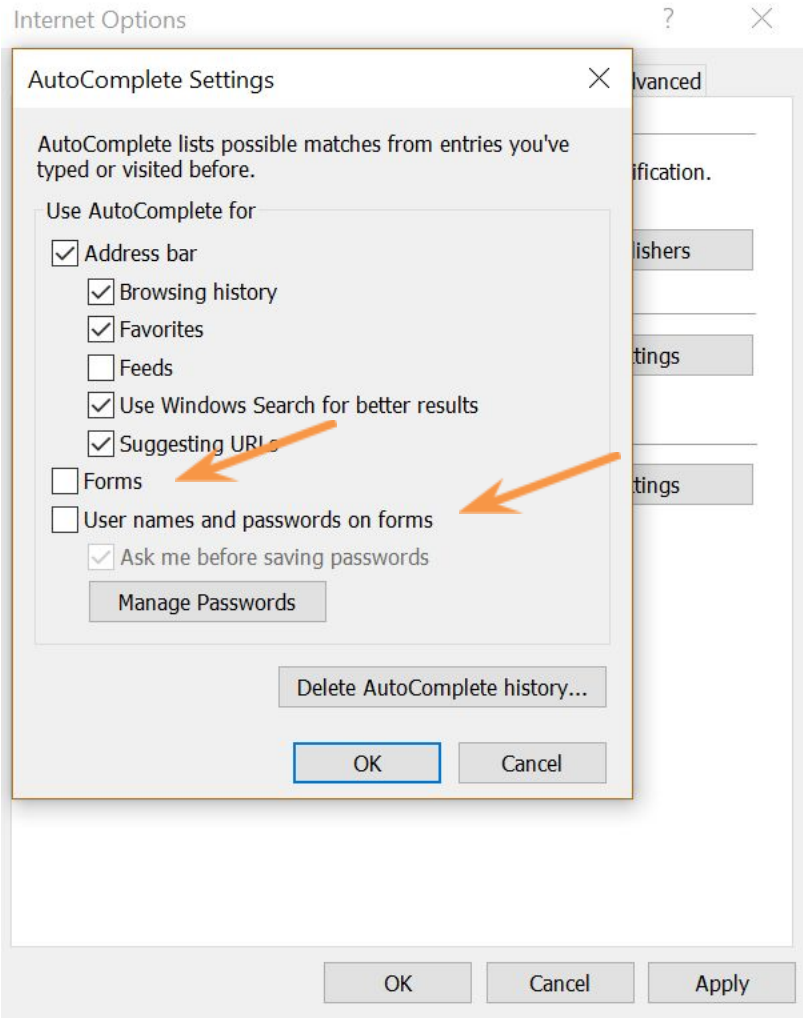
Step 3 – Enable ‘Delete browsing history on exit’, select ‘Apply’ then navigate to the ‘Content’ tab



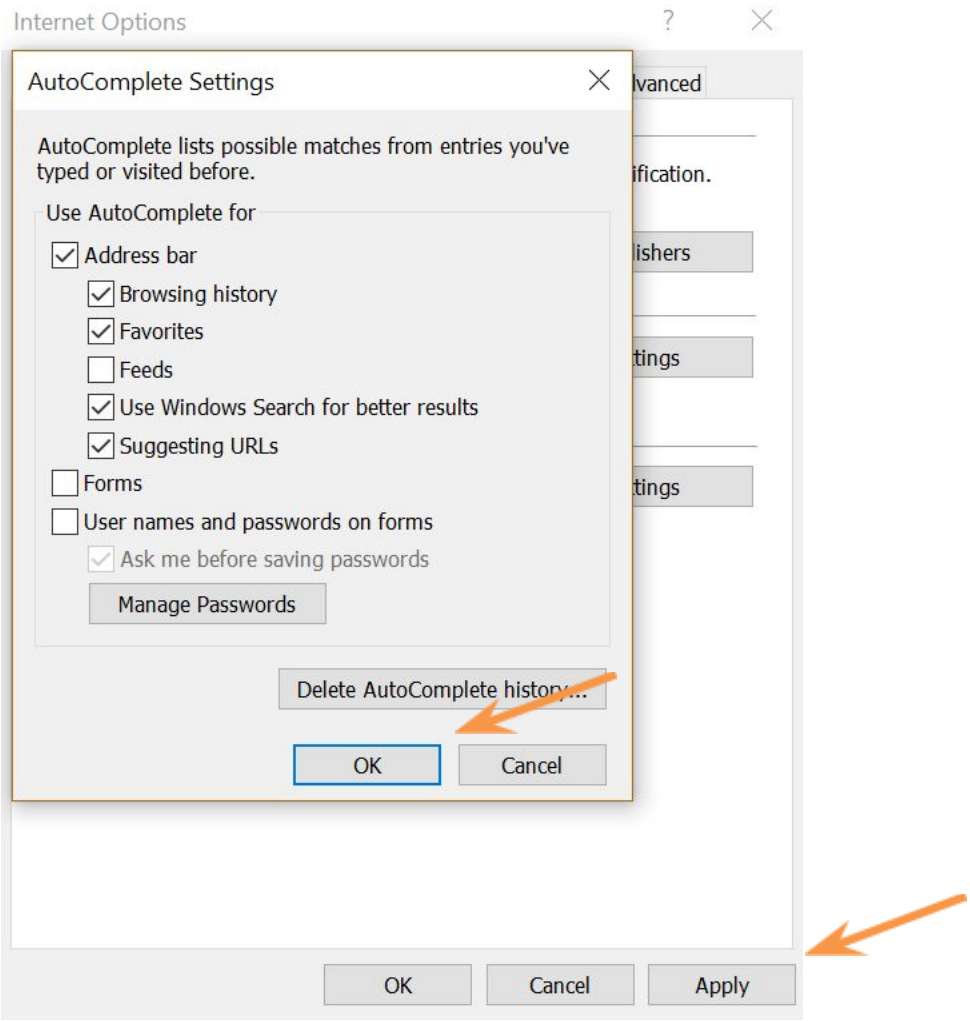
Step 4 – Select AutoComplete ‘Settings’



Step 4 – Disable AutoComplete for ‘Forms’ & ‘User names and passcodes on forms’

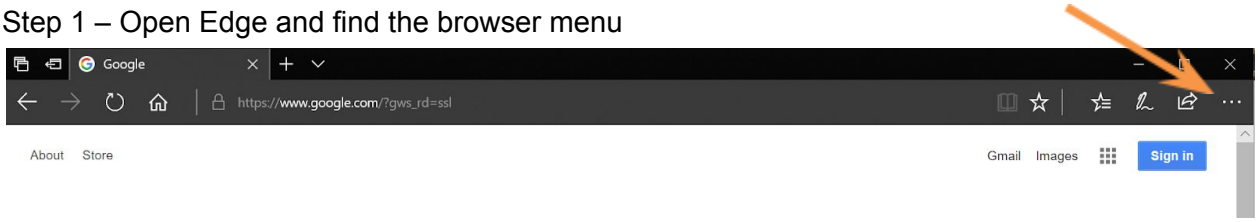


Step 5 – Select ‘OK’ then ‘Apply’

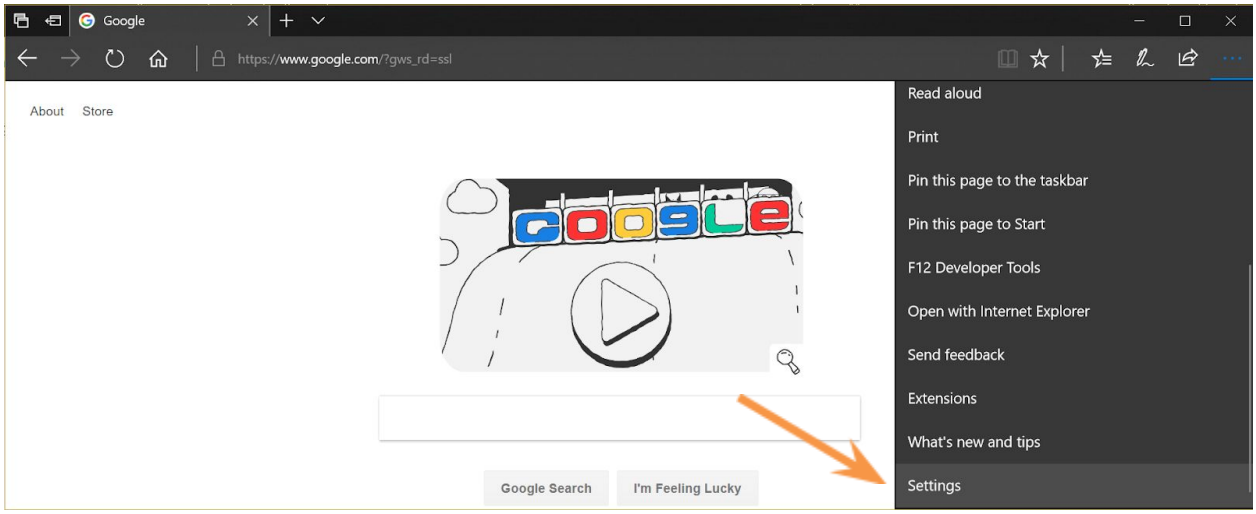


Edge (v41)

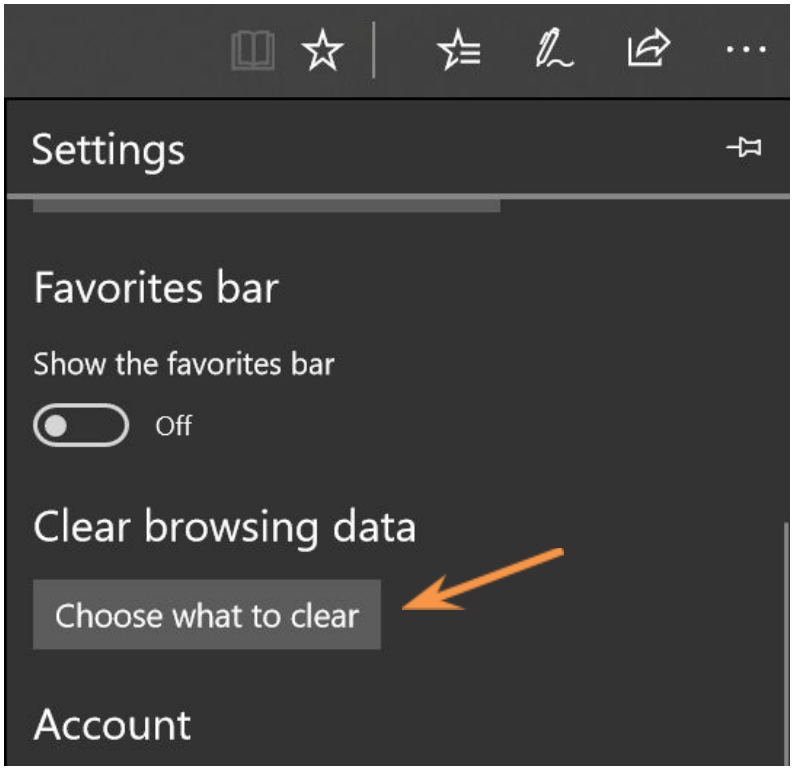
Step 1 – Open Edge and find the browser menu



Step 2 – Select ‘Settings’

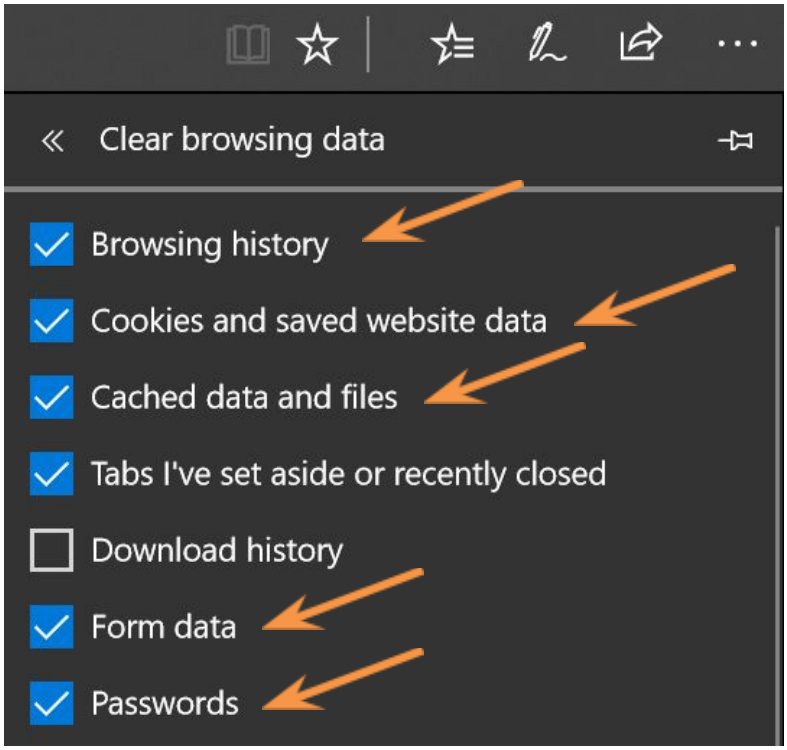


Step 3 – Under ‘Clear browsing data’ select ‘Choose what to clear’

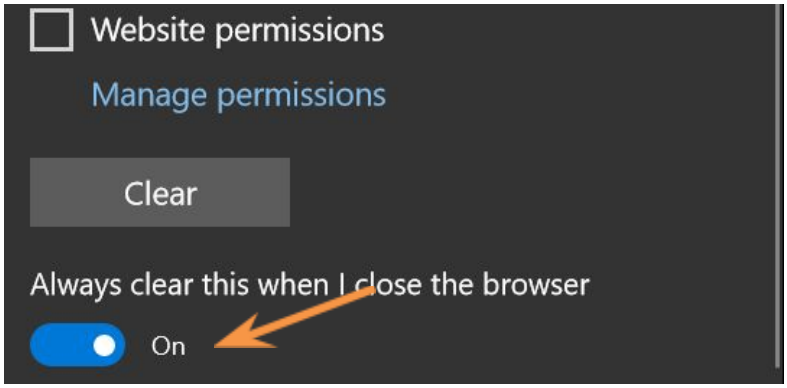


Step 4 – Make sure the following are checked:

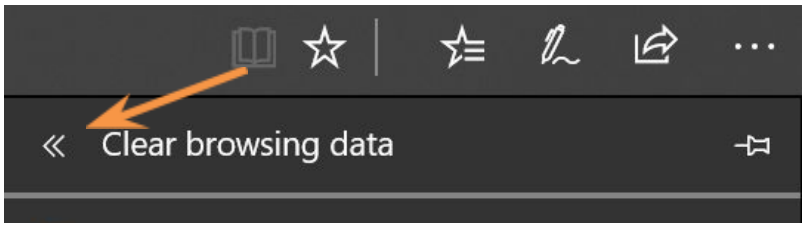
- Browsing history
- Cookies and saved website data
- Cached data and files
- Form data
- Passwords



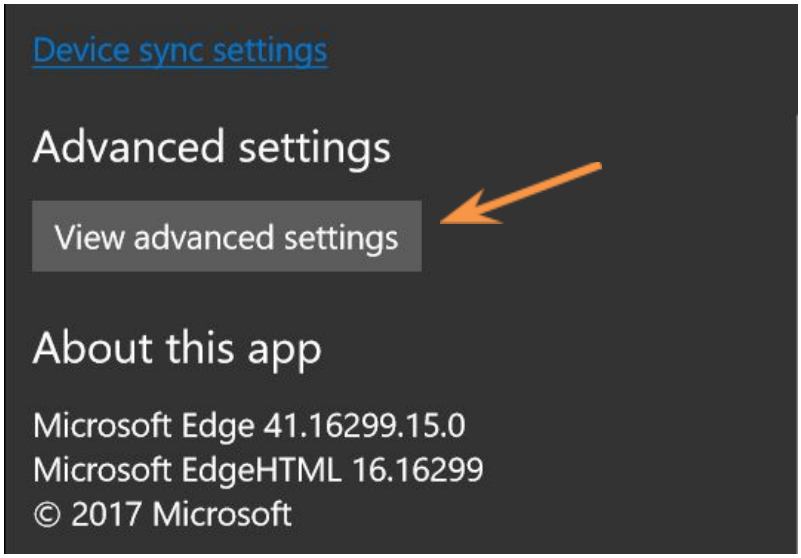
Step 5 - Turn on ‘Always clear this when I close the browser.



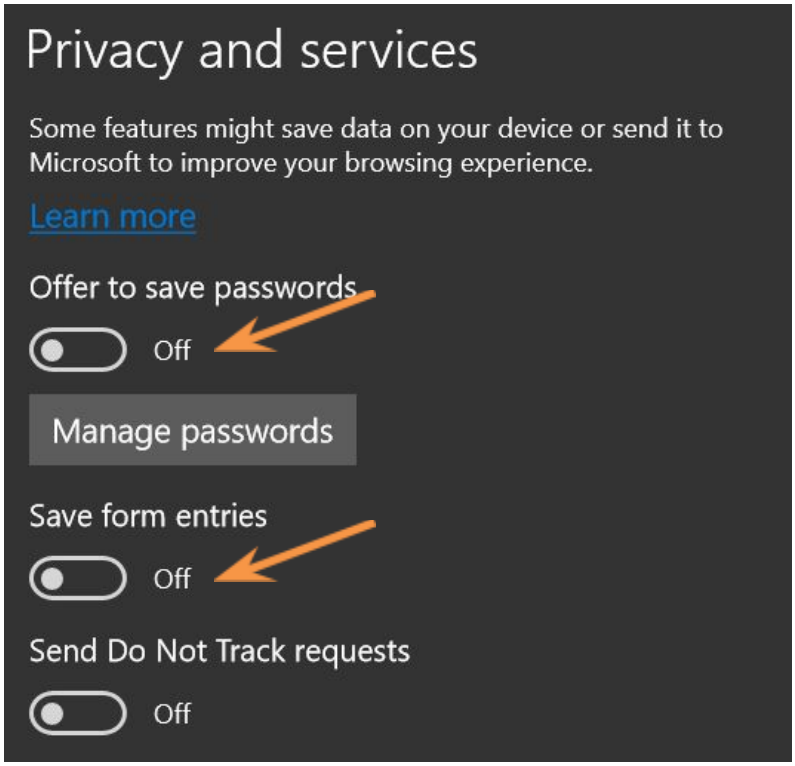
Step 5 – Navigate back to the previous menu



Step 6 – Select ‘View advanced settings’ near the bottom.

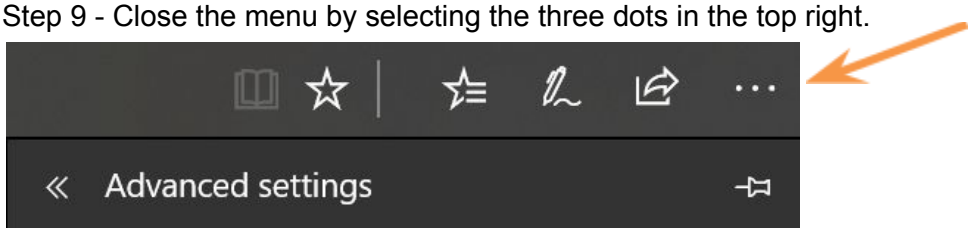


Step 7 – Scroll down to Privacy and services. Turn off ‘Offer to save passwords’ and ‘Save form entries’.



Step 8 - Scroll down to Cookies and set the dropdown box to ‘Don’t block cookies’.

Step 9 - Close the menu by selecting the three dots in the top right.



Configuring Mac OS X for Online Testing

This section describes how to configure Mac OS X for online testing.

Disabling Look-Up Gesture

Mac OS X versions 10.7 and later include a look-up gesture; highlighting a word and then tapping with three fingers on the trackpad displays a dictionary for the highlighted word—a feature that can compromise testing security. This section describes how to disable the look-up gesture.
The following instructions are based on mac OS X 10.9; similar instructions apply for other versions of mac OS X.

To disable the look-up gesture:

1. Choose Apple menu > System Preferences.
2. Click Trackpad. The Trackpad window opens.
3. Click the Point and Click tab.
4. Clear the Look up checkbox.

Disabling Display of Notification Center

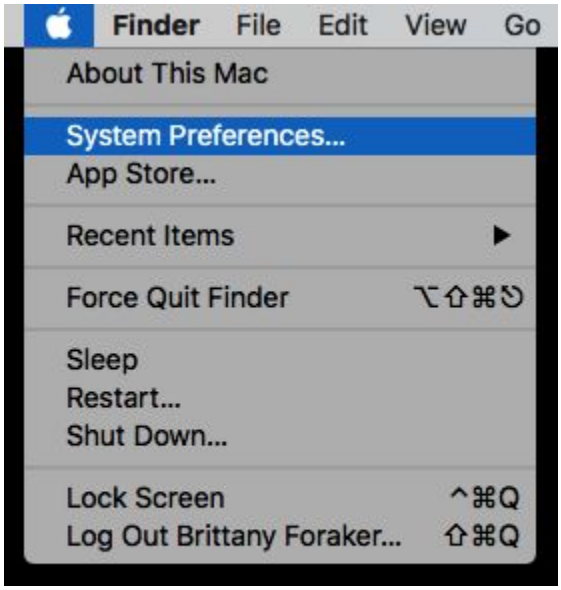
Mac OS X versions 10.10 and later include Notification Center, which displays system information when swiping to the left with two fingers from the right edge of the trackpad. Depending on its contents, Notification Center can compromise testing security. This section describes how to disable the gesture for displaying Notification Center.
The following instructions are based on mac OS X 10.10; similar instructions apply for later versions of mac OS X.

To disable the gesture for displaying Notification Center:

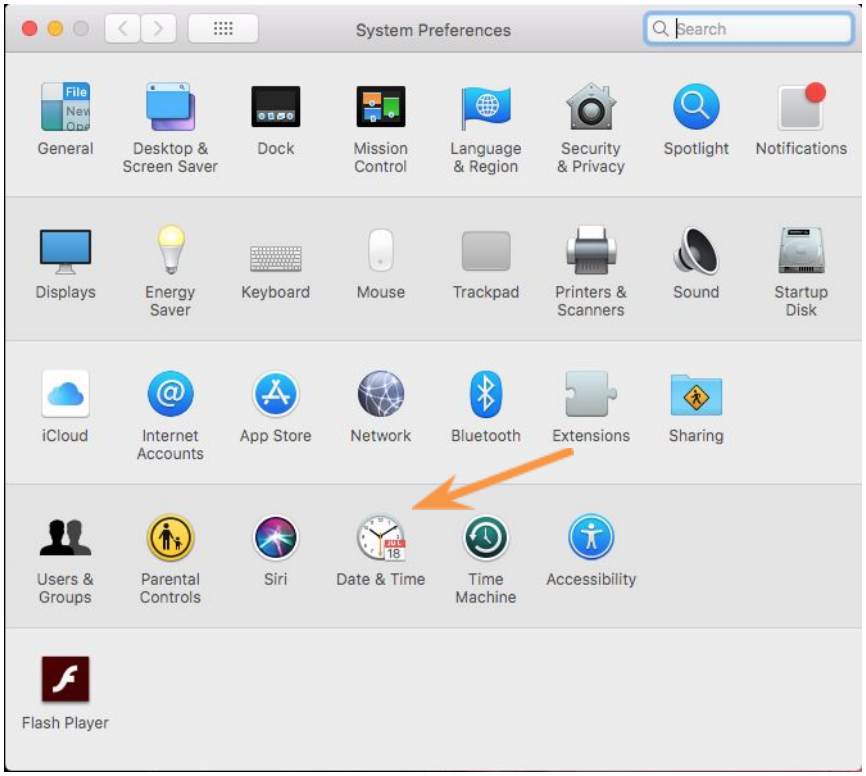
1. Choose Apple menu > System Preferences.
2. Click Trackpad. The Trackpad window opens.
3. Click the More Gestures tab.
4. Clear the Notification Center checkbox.

Syncing Computer Clock (High Sierra 10.13)

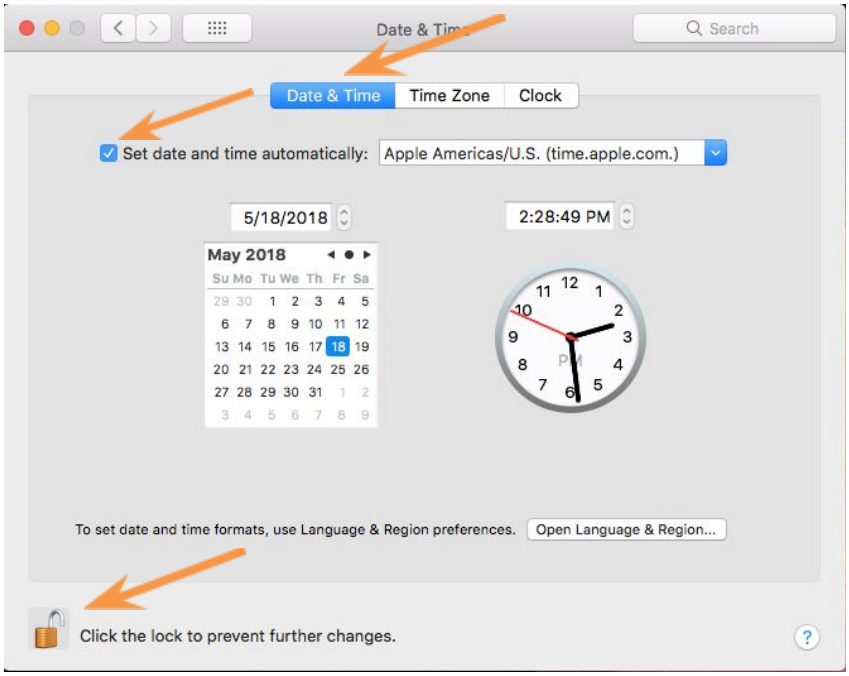
Step 1 - Choose the Apple menu > System Preferences



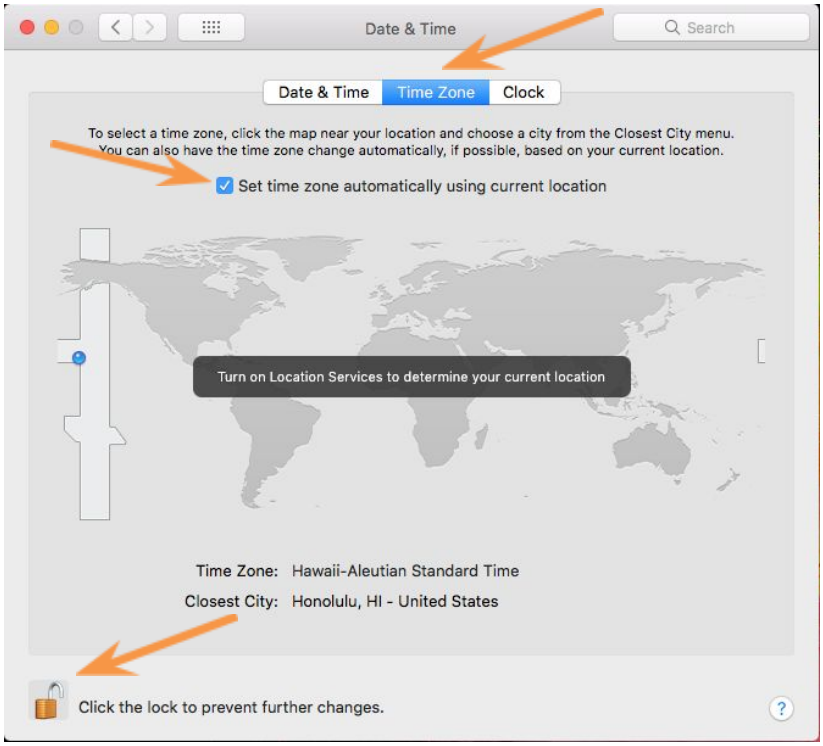
Step 2 - Select ‘Date & Time’



Step 2 - Click ‘Date & Time’, then set the date and time automatically. Note you made need to unlock the page in the bottom left before this feature can be turned on.



Step 3 - Select ‘Time Zone’, then enable ‘Set time zone automatically using current location’ or manually to ‘Hawaii-Aleutian Standard Time’



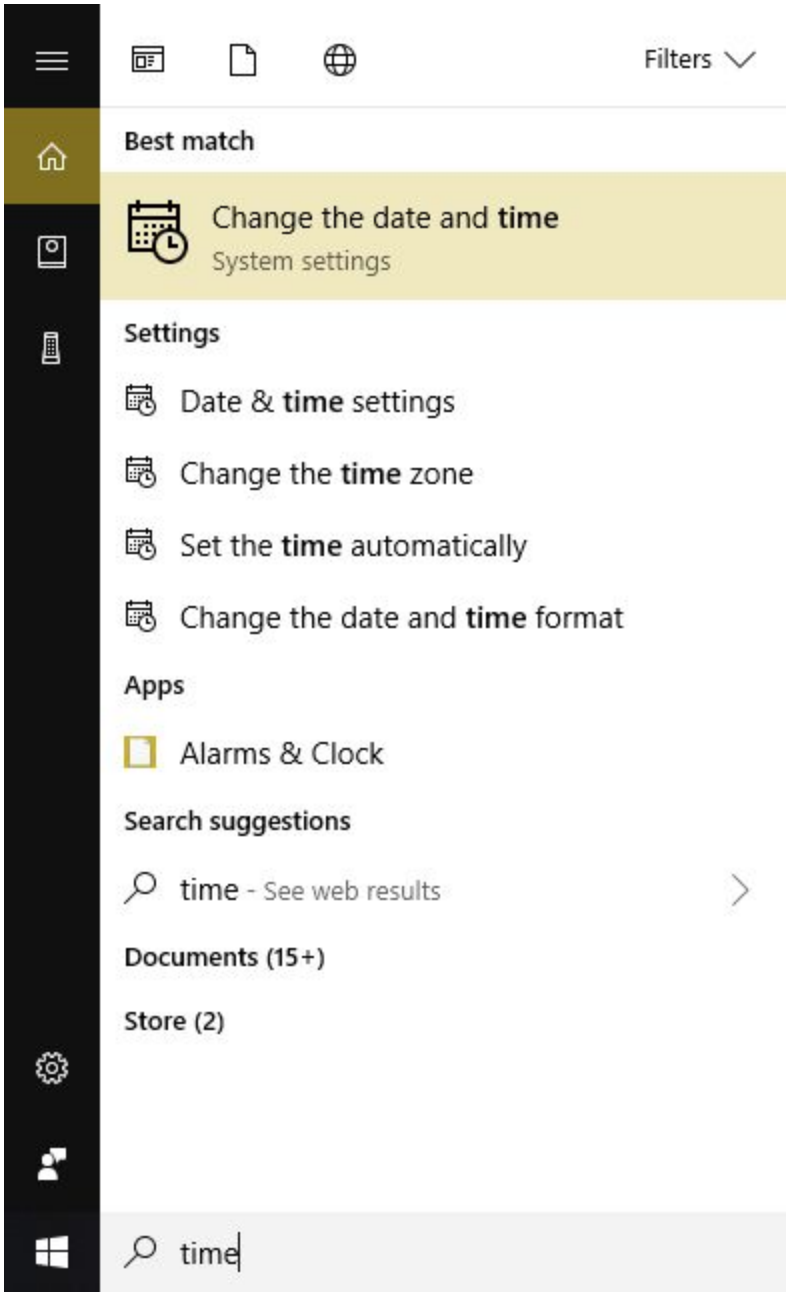
Configuring Windows for Online Testing

This section describes how to configure Mac OS X for online testing.

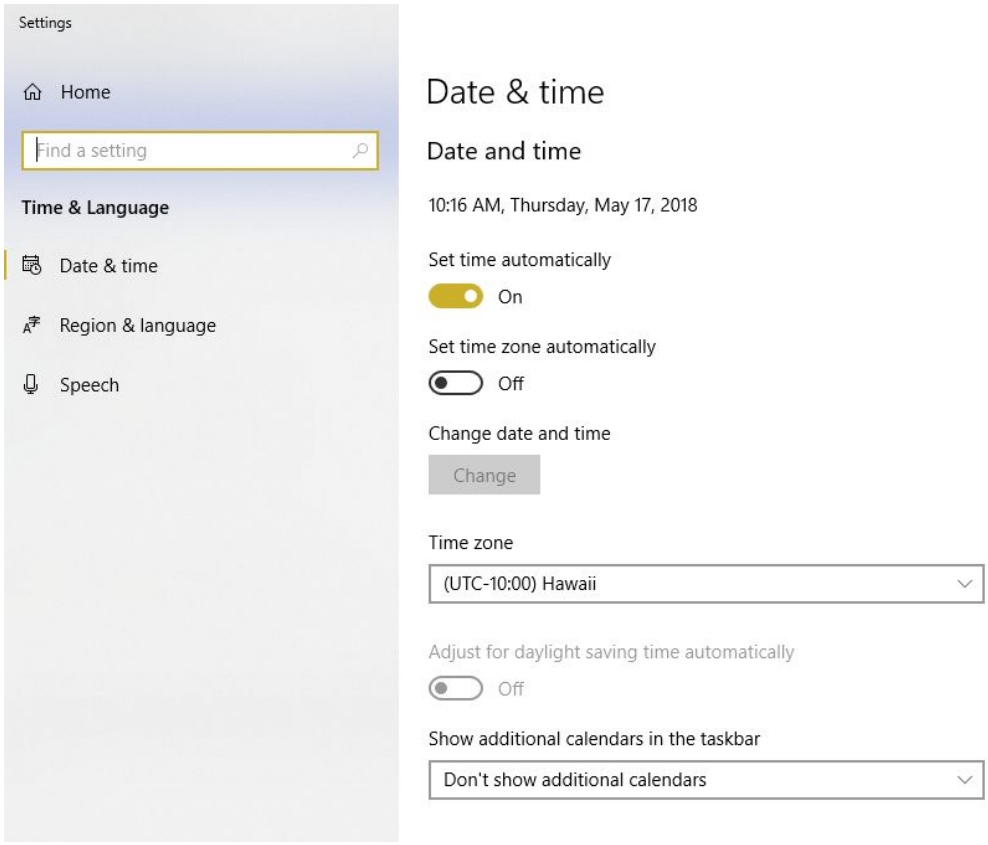
Syncing Computer Clock (Windows 10)

Step 1 - Using the search bar, type in ‘time’

Step 2 - Select ‘Change the date and time’



Step 3 - Turn on ‘Set time automatically’ and ensure ‘Time Zone’ is set to ‘(UTC-10:00) Hawaii’


Settings
Home
Find a setting
Time & Language
Date & time
Region & language
Speech
Date & time
Date and time
10:16 AM, Thursday, May 17, 2018
Set time automatically
On
Set time zone automatically
Off
Change date and time
Change
Time zone
(UTC-10:00) Hawaii
Adjust for daylight saving time automatically
Off
Show additional calendars in the taskbar
Don't show additional calendars

Appendix A. URLs Provided by KĀʻEO

This appendix presents information about the URLs used by KĀʻEO. Ensure your network's firewalls and filtering software are configured to allow access to these URLs.

URLs for Testing Site

kaiapuni.coe.hawaii.edu

URLs for Test Administrators

kaiapuni-wp.coe.hawaii.edu

Appendix B. Technology Coordinator Checklist

This checklist can be printed out referred to during review of networks and computers used for testing.

	Activity	Target Completion Date (Suggested: before school begins test administration)	Reference
☐	Verify that your school's network and Internet are properly configured for testing, conduct network diagnostics, and resolve any issues.		
☐	Verify testing devices meet the operating system requirements.		Appendix D
☐	Verify testing devices meet the web browser requirements.		Appendix D
☐	Verify testing devices meet the peripheral equipment requirements.		Appendix D
☐			
☐			

Appendix C. User Support

The testing program has established a Help Desk that is staffed by English and Hawaiian speakers. The Help Desk will be staffed Monday through Friday 8:00AM to 2:30PM (with the exception of University of Hawai‘i holidays). Help Desk staff will respond to your questions as quickly as possible. These personnel are trained to address your questions about aspects of the test administration both technical and logistical.

- The Help Desk phone number is: 808-956-7834
- The Help Desk email is: kaiapuni@hawaii.edu
- The website is: https://kaiapuni-wp.coe.hawaii.edu/kumu

Physical Address:
Hawaiian Immersion Assessment Project
Attn: Pōhai Kukea Shultz
1776 University Avenue, Everly 126
Honolulu, HI 96822

For questions about the content and purpose of the 2017 Hawaiian Immersion Assessment Project, please visit our website at: https://kaiapuni-wp.coe.hawaii.edu/kumu or contact the project staff at the University of Hawai‘i, Mānoa: kaiapuni@hawaii.edu.

Appendix D. Online System Requirements for KĀʻEO Testing

This document contains basic technology requirements for online testing for the Hawaiian Immersion Assessment Project tests for the 2019 administration. This document contains the following sections:

1. Supported Operating Systems for Student Testing
2. Supported Web Browsers for Online Systems
3. Requirements for Peripheral Equipment

The Test Administration Guide, this information, and other information related to the Hawaiian Immersion Assessment Project tests can be found at https://kaiapuni-wp.coe.hawaii.edu/kumu.

SUPPORTED OPERATING SYSTEMS FOR STUDENT TESTING

This section describes the supported operating systems for online testing.

Warning: Support for New Desktop Operating Systems
Operating systems that become available but do not appear in the following tables are not supported. Do not upgrade to new operating systems on computers that will be used to administer online assessments without ensuring the updates meet the required specifications

Desktops and laptops
The table below lists the operating systems and hardware required for student testing. Tablets and Chromebooks are not supported at this time. Online testing functions effectively with the minimum requirements listed. However, the recommended specifications provide improved performance.

Supported Operating Systems	Minimum Requirements	Recommended Specifications

Windows 7, 8.0, 8.1, 10	Pentium 4 or newer processor that supports SSE2 512 MB of RAM 200 MB of hard drive space	Core 2 or newer processor that supports SSE2 2+ GB RAM 80+ GB hard drive
Mac OS X (Intel) 10.6.x – 10.14.x	Intel x86 processor 1GB of RAM 10 GB hard drive	Intel x86 processor 2+ GB RAM 80+ GB hard drive

SUPPORTED WEB BROWSERS FOR ONLINE SYSTEMS

This section lists the supported web browsers for the 2017-2018 assessment. The table below lists the supported operating systems and corresponding web browsers for each Hawaiian Immersion Assessment Project application. It is recommended that schools use recent versions of supported web browsers. Each application requires disabling pop-up blocking software and enabling JavaScript. Be sure to use the correct combination of operating system and web browser. For example, Windows 8 requires Internet Explorer 10 or 11.

Supported Operating Systems	Supported Devices	Supported Browsers
Mac OS X		
10.6	Desktops, laptops	Chrome 31 or later, Firefox 35 or later
10.7	Desktops, laptops	Chrome 31 or later, Firefox 35 or later
10.8	Desktops, laptops	Chrome 31 or later, Firefox 35 or later
10.9	Desktops, laptops	Chrome 31 or later, Firefox 35 or later
10.10	Desktops, laptops	Chrome 31 or later, Firefox 35 or later
10.11	Desktops, laptops	Chrome 31 or later, Firefox 35 or later

10.12	Desktops, laptops	Chrome 31 or later, Firefox 35 or later
10.13	Desktops, laptops	Chrome 31 or later, Firefox 35 or later
10.14	Desktops, laptops	Chrome 31 or later, Firefox 35 or later
Windows		
7	Desktops, laptops	Chrome 31 or later, Firefox 35 or later, Internet Explorer 10–11
8.0	Desktops, laptops	Chrome 31 or later, Firefox 35 or later, Internet Explorer 10–11
8.1	Desktops, laptops	Chrome 31 or later, Firefox 35 or later, Internet Explorer 10–11
10	Desktops, laptops	Chrome 31 or later, Firefox 35 or later, Internet Explorer 10–11, Edge 25.10586 or later

REQUIREMENTS FOR PERIPHERAL EQUIPMENT

This section describes the requirements for peripheral equipment: screens, keyboards, and headphones.

Screen resolution requirements
All devices must meet the following minimum resolution. Larger resolutions can be applied as appropriate for the monitor or screen being used.

Desktops and laptops must have 1024 x 768 minimum resolution.

Depending on the screen size, students may need to use vertical or horizontal scroll bars to view all test-related information. Students may also use the Zoom tool through their web browser to enlarge the content on the screen.

Keyboards

The use of a physically connected keyboard is required for testing. Students may use a built-in keyboard, such as on a laptop, or regular external keyboard attached via a physical connector (USB, PS/2). Wireless (either via wireless adapter or Bluetooth) keyboards are not supported. In the case where accommodations are necessary, an on-screen keyboard may be utilized, but is not recommended for general use.
Some external keyboards have additional “shortcut” buttons that can create security issues. These buttons may allow students to open another application. It is strongly recommended that students do not use these kinds of keyboards that have these shortcut buttons. In addition, students will be able to type their answers using a Hawaiian keyboard in order to insert diacritical markings. If the computer does not have the Hawaiian keyboard, students can use on-screen input buttons on the assessment to insert diacritical markings onto their writing.

Headphones
Students will need headphones to listen to audio for the Hawaiian Language Arts and Science online assessments.

- Students with the text-to-speech feature can listen to stimuli or test items being read aloud.
- Students with the enhanced accessibility mode feature can use the Job Access with Speech (JAWS®) or other similar screen reading software.

Test Coordinators should determine how many students will need headphones prior to testing to ensure that there is an adequate supply on hand.

The following headphones are supported:

- Wired headphones with a 3.5 mm connector.
- The following Bluetooth headphones: Logitech H800, SoundBot SB270, and ECO Sound ECO-V300.
- Wired headphones with a 3.5 mm connector or USB headphones (wired or wireless) are recommended over Bluetooth, as they provide better clarity and accuracy.