Lippincott Procedures, Lippincott Advisor, Lippincott Professional Development Collection, and Lippincott Blended Learning
Browser Requirements and Network Best Practices

Revised 05/05/2020

Below is the current list of client requirements along with specific network requirements to support internet access from an institution to the Lippincott Solutions primary and disaster recovery (DR) server farms.

Proper and complete site operation requires these guidelines be implemented by the purchasing institution in the context of the network infrastructure and local desktop deployment environment.

Supported Web Browsers:

- Internet Explorer 10 if TLS 1.2 support is manually added
- Internet Explorer 11 or higher
- Microsoft Edge
- Firefox (current and previous 3 versions)
- Safari (current and previous version)
- Google Chrome (current and previous version)

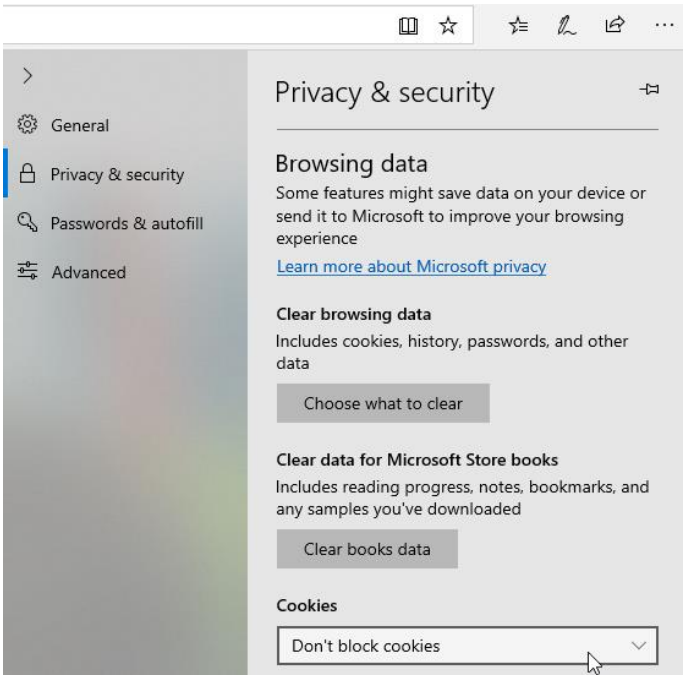
Supported Mobile Web Browsers:

- iPhone with iOS 8 or greater
- iPad with iOS 8 or greater
- Android devices with 4.4 or higher

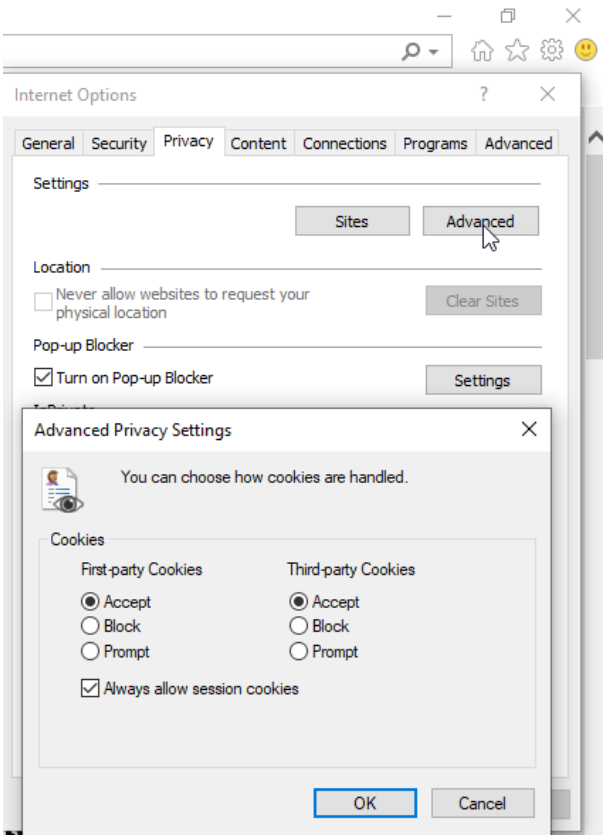
Local Web Browser Settings:

- Full JavaScript support in the browser ENABLED
- Cookies (session and disk) enabled if the facility shares the same IP as other facilities (for differentiation among these facilities)
- Cookies (session) enabled (ALWAYS)

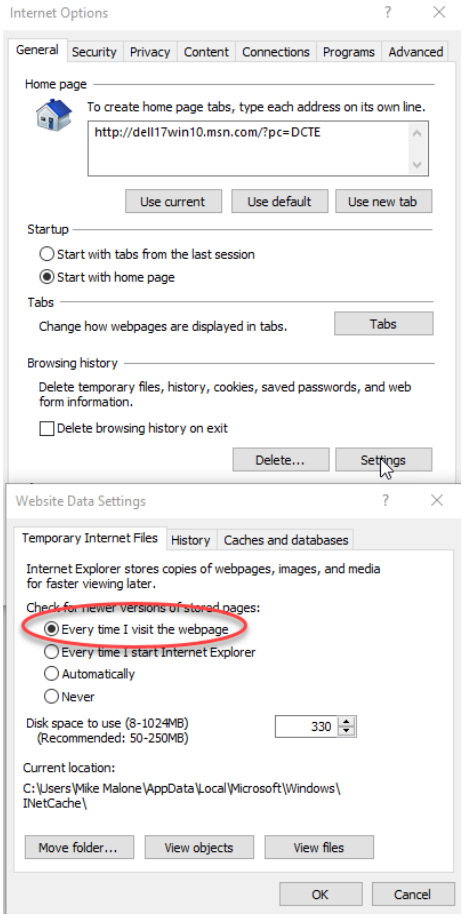
Cookie Settings (MS Edge Example – Settings | Privacy & Security):



Cookie Settings (IE 11 Example – Internet Options | Privacy):



- Temporary Internet Files (IE): Check for newer versions of stored pages setting: Every time I visit the page (Internet Options | Browsing History <Settings>



Web Browser Plug-in(s):

- Adobe PDF Reader - required to view PDFs: http://get.adobe.com/reader/

Networking / Security Hardware / Software

- Pop-ups NOT blocked by web browser or third-party security software such as Antivirus, Security Suites, Network or Personal Firewalls (Norton, MacAfee, Windows Firewall, Windows Defender, etc.)
- HTTP and HTTPS communication to https://procedures.lww.com, https://advisor.lww.com, https://advisor-edu.lww.com, https://competency.lww.com, https://blendedlearning.lww.com, https://lns-services.lww.com, and https://lns-security.lww.com unimpeded by network routers, firewalls, proxy servers
- HTTP and HTTPS communication to https://procedures.lww.com, https://advisor.lww.com, https://advisor-edu.lww.com, https://competency.lww.com, https://blendedlearning.lww.com, https://lns-services.lww.com, and https://lns-security.lww.com unimpeded by local security software such as Antivirus, Security Suites, Network or Personal Firewalls (Norton, MacAfee, Windows Firewall, Windows Defender, etc.). The specified site domain names *.lww.com and *.wkhpe.com should be "trusted" by any relevant security hardware or software.

- The Lippincott Nursing Solutions (LNS) platform no longer supports TLS 1.0 or TLS 1.1. All browsers and SSL communication must be TLS 1.2 compliant.

URL Information for Firewall/Proxy Administrators

Wolters Kluwer recommends that you allow users to connect to all *.lww.com and *.wkhpe.com domains, to ensure uninterrupted access for users. If that is not possible, we recommend that you allow access to the following service URLs, depending on which products you subscribe to.

Domain Names to Allow/Trust:

- *.lww.com
    - procedures.lww.com
    - dr-procedures.lww.com
    - images.procedures.lww.com
    - images.dr-procedures.com
    - downloads.lww.com
    - unavailable.procedures.lww.com
    - www.lww.com
    - advisor.lww.com
    - competency.lww.com
    - ceconnection.lww.com
    - blendedlearning.lww.com
    - lpd.lww.com
    - lns-media.lww.com
    - lns-services.lww.com
    - lns-security.lww.com
- *.wkhpe.com
    - ns-content-service.wkhpe.com
    - lns-media.wkhpe.com
- wolterskluwerhealth.d2.sc.omtrdc.net (Omniture Web Analytics)
- mobile-app users that have proxy-based access to the internet:
    - *.flurry.com
    - *.appcelerator.com

Network traffic between LNS products and your network

All network traffic from LNS products to your network should be in response to requests which users have generated. Please whitelist/allow all traffic without caching to the IPs: 69.84.140.124 and 69.84.140.125.

Please allow all traffic to the AWS CNAME ause1plnspubalb1-36870316.us-east-1.elb.amazonaws.com.
To ensure proper delivery of email, customers are encouraged to explicitly whitelist email domains: wolterskluwer.com, lww.com, wkhpe.com.