TLS v 1.2 update

Auto-Graphics is adopting StateRAMP cybersecurity policies and will require libraries to use Transport Layer Security (TLS) v 1.2 or greater by **Tuesday, November 5th, 2024,** to keep web browsing secure. Many software applications have required TLS v 1.2 for several years.

- Operating systems and browsers on each device could be using different TLS versions. We recommend checking a variety of devices if you suspect they may be running outdated operating systems or browsers.

- Staff can test if their device and browsers are supporting TLS v 1.2 by visiting:
  - https://sectest-rsdemo.agshareit.com
  - If the site loads, the device supports TLS v 1.2 or greater and no other action is needed.

- If staff cannot access the site, they will need to check with their IT department to be upgraded to TLS v 1.2 or greater or consult the instructions below.

Many modern browsers and operating systems already support TLS 1.2 by default, but these steps will guide you through checking and enabling it if necessary.

Instructions for upgrading

Browsers

Google Chrome (Windows, macOS, Linux)

1. Open Chrome: Launch the Chrome browser.
2. Check Chrome Version:
    - Click the three vertical dots (menu) in the upper-right corner.
    - Go to Help → About Google Chrome.
    - Ensure Chrome is version 29 or higher. If not, update Chrome because newer versions support TLS 1.2 by default.
3. Enable TLS 1.2 (if needed):
    - Type `chrome://flags` in the address bar and press Enter.
    - Search for TLS in the search box.
    - Ensure that TLS 1.2 or later is enabled.
4. Update Settings (if needed):
    - Go to Settings.
    - Under Privacy and Security, click on Security.
    - Ensure that Use Secure DNS is enabled.

Mozilla Firefox (Windows, macOS, Linux)

1. Open Firefox: Launch the Firefox browser.
2. Check Firefox Version:
    - Click the three horizontal lines (menu) in the upper-right corner.
    - Go to Help → About Firefox.
    - Make sure you're using Firefox version 27 or later, as it supports TLS 1.2 by default.
3. Enable TLS 1.2:
    - Type `about:config` in the address bar and press Enter.
    - If a warning message appears, click Accept the Risk and Continue.
    - Search for the preference `security.tls.version.min`.
    - Set the value to `3` (which corresponds to TLS 1.2).
4. Restart Firefox to apply changes.

Microsoft Edge (Windows, macOS)

1. Open Edge: Launch Microsoft Edge.
2. Check Edge Version:
    - Click the three horizontal dots (menu) in the upper-right corner.
    - Go to Help and Feedback → About Microsoft Edge.
    - Ensure Edge is updated to version 12 or later, as TLS 1.2 is enabled by default.
3. Check TLS Settings (if necessary):
    - Type `edge://flags` in the address bar and press Enter.
    - Search for TLS and ensure that TLS 1.2 is enabled.

Safari (macOS)

1. Open Safari: Launch Safari browser.
2. Check Safari Version:
    - Click Safari in the menu bar and select About Safari.
    - Ensure you are using Safari version 7 or later, as these versions support TLS 1.2 by default.
3. Enable TLS 1.2:
    - There is no need to manually enable TLS 1.2 in Safari as it's automatically supported on macOS 10.9 (Mavericks) or later.

Opera (Windows, macOS, Linux)

1. Open Opera: Launch the Opera browser.
2. Check Opera Version:
    - Click the Opera Menu in the upper-left corner.
    - Go to Help
    - Select About Opera.
    - Ensure you have version 17 or later, which supports TLS 1.2 by default.
3. Enable TLS 1.2 (if needed):
    - Type `opera://flags` in the address bar.
    - Search for TLS and verify that TLS 1.2 is enabled.

Internet Explorer (Windows)

1. Open Internet Explorer: Launch Internet Explorer.
2. Check IE Version:
    - Click the gear icon in the upper-right corner and select About Internet Explorer.
    - Ensure you are using IE version 11, as this version supports TLS 1.2 by default.
3. Enable TLS 1.2:
    - Click the gear icon and go to Internet Options.
    - Click the Advanced tab.
    - Scroll down to the Security section.
    - Check the box next to Use TLS 1.2.
    - Click Apply and OK.
4. Restart Internet Explorer to apply the changes.

Operating Systems

Windows 7 and Above

1. Open the Control Panel: Go to Start → Control Panel.
2. Navigate to Internet Options:
    - Click Network and Internet → Internet Options.
    - Select the Advanced tab.
3. Enable TLS 1.2:
    - Scroll down to the Security section.
    - Check the boxes for Use TLS 1.2 (also, optionally check Use TLS 1.3 for futureproofing).
    - Click Apply and OK.
4. Reboot the system for the changes to take effect.

macOS 10.9 Mavericks and Above

TLS 1.2 is enabled by default on macOS 10.9 and later, and no manual steps are required to enable it.

Linux

Most modern Linux distributions support TLS 1.2 out of the box, provided that you are using up-to-date versions of browsers like Chrome, Firefox, or Opera. Ensure that OpenSSL is updated to a version supporting TLS 1.2.

1. Update OpenSSL:
    - Open a terminal and run:
    - ```bash
    - sudo apt-get update
    - sudo apt-get upgrade openssl
    a. ```
2. Verify TLS 1.2 Support:
    - You can verify support for TLS 1.2 by running:
    - ```bash
    - openssl s_client -connect google.com:443 -tls1_2
    - ```
3. If successful, this confirms that your system supports TLS 1.2.

Communication with IT

If staff find they are not able to access the link or update the TLS version with the instructions above, we recommend contacting the IT department of your library for next steps. Here is an example of how you can start the conversation.

Subject: Request to Verify TLS 1.2 Support

I received a URL from one of our vendors to verify that my computer and browser are configured to support TLS 1.2, as this is required to access their service securely. I was not able to access the provided link. Could you please assist with the following?

1. *Test URL:*
   - *This is the URL provided to check whether I can establish a secure TLS 1.2 connection https://sectest-rsdemo.agshareit.com.*
2. *Check TLS 1.2 Compatibility:*
   - *Ensure that both my computer and browser are configured to support at least TLS 1.2.*
   - *Review and confirm the appropriate security protocols are enabled in the browser settings (e.g., Google Chrome, Firefox, Microsoft Edge, etc.).*
3. *Update System or Browser Settings (if needed):*
   - *If TLS 1.2 is not enabled, please update the settings on my system or browser to ensure compliance with the vendor's requirements, and check the provided link again.*

Please let me know once the test is complete or if further steps are necessary.

Auto-Graphics Customer Support

If none of the above actions have worked or you have questions about this upgrade, please contact your VERSO or SHAREit system administrator. You may also contact A-G customer support directly if needed.

Customer Support Web Portal
https://auto-graphics.atlassian.net/servicedesk/customer/portals

Call (800) 852-8686
Monday - Friday, 8 a.m. - 8 p.m. Eastern

Email
helpdesk@auto-graphics.com