

Clearing Your Cache\Delete Cookies in Internet Explorer 10.0 or higher

- Log out of Integrity's website and close all other browser tabs\windows.
- Select Tools – Internet Options



- Click on the General Tab-Browsing History and select Delete and the Delete Browsing History screen will appear.
- Check the Temporary Files Files, Cookies and History Boxes and make sure all other boxes are unchecked.
- Select Delete



- Close Internet Explorer and re-open. Log back into Integrity's website and re-enter your username and password, do not use save information.

TLS1.0 Support Stopping on June 29, 2016

Our current web ordering site(s) ECinteractive and ECinteractivePLUS will be ending support of TLS1.0 on **February 27, 2016**. Any browsers with TLS1.0 enabled need to be updated to continue accessing web storefronts after February 27, 2016. For more information about this change, please see below.

What is TLS?

[TLS \(transport layer security\)](#) is a cryptographic protocol designed for communication security. TLS is used in many applications, including browsers.

Why are we ending support?

To remain PCI compliant, monthly scans must be performed by a Qualified Security Assessor (QSA). These scans check many different parts of the software, including hardware, security, etc. Scans are now detecting support for TLS1.0, and support for TLS1.0 means an immediate failure. Effective June 30, 2016, any system supporting TLS1.0 will no longer be able to accept credit card transactions.

What do I need to do before February 27, 2016?

As a customer, you need to do three things:

1. Make sure you aren't using a browser with only TLS1.0 enabled. Use the bullets below to update your browser.
 - O If you are using XP or Vista, you must use Firefox or Chrome.
 - O If you are using Firefox or Chrome, make sure your browser is updated to the latest version. We recommend updating anytime a new version is available.
 - O If you are using Internet Explorer version 8-10 on Windows 7 or 9, make sure TLS1.2 is enabled under Advanced Settings.
 - O If you are using Internet Explorer version 9-v11, check your settings to ensure TLS1.0 isn't checked and TLS1.2 is checked.
2. Oracle, Peoplesoft, Sciquest, and Ariba all support TLS1.1 and TLS1.2. If you are using a punch-out not listed above, contact your customer and/or punch-out vendor to alert them of this change.

You may need to contact your IT staff if you are not allowed to make these needed changes listed above. These changes will need to be done for all computers that are being used to access ECinteractive, ECinteractivePLUS, DForce2, and DForce2PLUS.

What happens if I don't make this change before February 27, 2016?

You will not be able to access our web storefront until you update your browser.

I need TLS1.0 for other websites what are my options?

If you have websites that are still requiring you to use TLS1.0 you can either toggle this setting on and off as you access these sites in the setting of Internet Explorer OR you can use Chrome or Firefox to access ECinteractive, ECinteractivePLUS, DForce2, and DForce2PLUS. Please contact your internal IT staff if you have additional questions.