PCI Requirements for Transport Layer Security (TLS) 1.2
Changes coming to Access Online will require your immediate attention. The Payment Card Industry Data Security Standard (PCI DSS) requires that the Secure Sockets Layer (SSL) and early versions of Transport Layer Security (TLS) be disabled by May 30, 2018. To be fully compliant with the PCI directive, Access Online will disable all support for older operating systems and web browsers that use TLS 1.0 and 1.1 on or before May 30, 2018. Clients who choose to maintain older operating systems and/or browsers after this date (or are unable to upgrade their operating system to allow use of a supported browser), will no longer be able to access our web-based solutions, including Access Online.

SSL and TLS are cryptographic protocols that provide communications security over computer networks. Websites are able to use these protocols to secure communications between their servers and web browsers.

Every website that transmits or processes credit card data will make this change prior to June 30, 2018. You are receiving this notification to ensure your organization continues to have access to Access Online. Access Online is hosted by U.S. Bank and we are committed to protecting your data and continue to take the necessary steps to keep the network safe.

Why?
Earlier versions of encryption protocols used to transport data securely between a client and a server (SSL, TLS 1.0 and TLS 1.1) no longer meet minimum standards with industry best practices for security and data integrity. The PCI Security Standards Council (SSC) have explicitly advised that these protocols must be disabled. Moving forward, only TLS version 1.2 or higher will be considered strong cryptography, and can be used as a security control to protect Cardholder Data environments after May 30, 2018.

When?
In order to be fully compliant with the PCI SSC directive, and to allow time to collect evidence of the disablement of insecure protocols, Access Online will disable all support for TLS 1.0 and 1.1 on or before May 30, 2018. After that date, any attempt to utilize Access Online in a browser without TLS 1.2 enabled will be rejected.

How to avoid disruption?
- If your systems and browsers currently support TLS 1.2 but it has been disabled or has not been enabled, access the security settings in the browsers to enable TLS 1.2.
- If your systems and browsers currently do not support TLS 1.2, you will need to install the appropriate Operating System and/or web browser, then ensure that TLS 1.2 has been enabled in the browser(s).
- If your organization uses Webservices to connect to Access Online, you will need to install the appropriate Server and Operating System(s).
How do I know if my browsers and/or operating systems are TLS 1.2 compatible?

- Determine what versions of Operating System, web server/browser or framework your application runs on? To test, you would enable TLS 1.2, and disable TLS 1.0 and 1.1. See below the Operating System versions, Web Browsers, Application & Frameworks.

### Workstation and Server Operating System Versions

<table>
<thead>
<tr>
<th>Workstation and Server Operating System Versions*</th>
<th>Web Browsers</th>
<th>Applications, Utilities and Frameworks*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 7</td>
<td>Internet Explorer v11+ **</td>
<td>OpenSSL 1.01+</td>
</tr>
<tr>
<td>Windows 8</td>
<td>Microsoft Edge</td>
<td>JDK 8 +</td>
</tr>
<tr>
<td>Windows 8.1</td>
<td>Google Chrome v30+</td>
<td>.NET 4.6 +</td>
</tr>
<tr>
<td>Windows 10</td>
<td>Mozilla Firefox v27+</td>
<td>Apache 2.2.23</td>
</tr>
<tr>
<td>Mac OS X 10.9 +</td>
<td>Apple Safari v7+</td>
<td></td>
</tr>
<tr>
<td>iOS 5.x +</td>
<td>Opera v17+</td>
<td></td>
</tr>
<tr>
<td>Android 5.x +</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows Server 2012</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows Server 2012 R2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows Server 2016</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows Server 2008 R2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CentOS 6+ / RHEL 6+ (Linux)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* The Operating Systems will require the minimum version of web browser or application, as listed above, to be compatible. **Server Operating System versions and Applications, Utilities and Frameworks** information is only applicable if your organization connects to Access Online using Webservices like API calls, XML calls, SFTP servers and/or Batch Servers.

** Internet Explorer 11 is the recommended browser version and has TLS 1.2 enabled by default. IE 9 and 10 may potentially work but are still prone to security risks and we cannot guarantee the browser behavior. Microsoft no longer supports Internet Explorer versions older than IE 11. This means these versions are no longer receiving security updates. For more information please refer to the [Microsoft Internet Explorer Life Cycle page](https://www.microsoft.com/en-us/software/internet-explorer/lifecycle).

### How do I find my browser version?

- **Microsoft Internet Explorer** - browser version should be IE 11 or later
  From the IE menu bar, click **Help** and select About Internet Explorer.

- **Google Chrome** - browser version should be Chrome 40.0.2214 or later.
  Launch Chrome, click **Customize and control Google Chrome** (the wrench icon) and then select **About Google Chrome**.

- **Mozilla Firefox** - browser version should be Firefox 31.4.0 or later.
  From the Firefox menu bar, click **Help** and then select About Mozilla Firefox.

- **Apple Safari** - browser version should be Safari 7 or later.
  Launch Safari, click **Display a menu of general Safari settings** (gear icon), and select **About Safari**.
Communication channels to consider when determining if your integration supports TLS 1.2
(only applicable if your organization utilizes Webservices to connect to Access Online; not applicable if only using Access Online by logging into the system through our website):

- **.NET**
  - .NET 4.6 uses TLS 1.2 automatically.
  - .NET 4.5 can be configured to use TLS 1.2.
  - .NET 3 and below does not support TLS 1.2.

- **Java**
  - Java 8 supports TLS 1.2 and enables its use by default
  - Java 7 supports TLS 1.2, but does not enable its use by default for clients.
  - Java 6 does not support TLS 1.2 natively, but support for TLS 1.2 in Java 6 is provided by third parties.

- **OpenSSL (PHP, Ruby, Python)**
  - Most dynamic languages such as Ruby, PHP, and Python rely on the underlying operating system's OpenSSL version. You can check it by running the command 'openssl version'. 1.0.1 is the minimum version required.

**What are some Tips for a Successful TLS Upgrade?**

- Use an up-to-date operating system. Some older OS require a registry change before software will even attempt to make a TLS 1.2 connection.
  - Note: Enabling TLS 1.2 at the OS level is not usually sufficient to fix old code; typically, old code will need to be updated.

- If using Webservices to connect to Access Online (API calls, XML calls, SFTP servers and/or Batch Servers):
  - Ensure your scripting language is compatible with TLS 1.2.
  - Many older versions require specific commands to enable TLS 1.2.
  - Some languages may have bugs preventing SSL negotiations to connect with TLS 1.2, even with it enabled and set as preferred.
  - Confirm your HTTPS library (e.g. OpenSSL) supports TLS 1.2. Some older libraries may not support TLS 1.2 and need to be upgraded or require TLS 1.2 to be selectively enabled.

**How do I enable TLS 1.2 in my browser?**

To check your version and enable TLS 1.2 protocols on your web browser ONLY, see below, you may need to contact your IT department or Administrator to make this security change on your browser. If you have other connections, API calls, XML calls, SFTP servers and/or Batch Servers, use the minimum requirements listed for Servers and/or Applications in the table above to check your current environments.

Most of the supported browsers listed above have TLS 1.2 enabled by default. If a user utilizes a browser other than those listed above or has tampered with the default settings here is a list of steps to support enabling TLS 1.2 in various browsers:
Microsoft Internet Explorer 11
- From the menu bar, click Tools>Internet Options
- Click on the Advanced Tab
- Scroll down to the Security section where you can see the TLS versions selected.
- Click OK.
- Close your browser and restart Internet Explorer.

Google Chrome
- Open Google Chrome
- Click the options menu in the top right
- Click the Settings Option
- Click the Show Advanced Settings at the bottom of the page
- Scroll down to Network section and click Change Proxy Settings. (You may need to contact your IT department)
- Select Advanced Tab
- Scroll down to Security category, manually check the option box for TLS 1.2

Mozilla Firefox
- Open Firefox
- In the address bar, type about:config and press Enter
- In the Search field enter tls. Find and double-click the entry for security.tls.version.min
- Set the integer value to "3" to force a minimum protocol of TLS 1.2
- Click OK.
- Close your browser and restart Google Chrome

**Opera**
- Open Opera.
- Click Ctrl plus F12.
- Scroll down to the Network section and click on Change proxy settings.
- Select the Advanced tab.
- Scroll down to Security category, manually check the option box for Use TLS 1.1 and Use TLS 1.2.
- Click OK.
- Close your browser and restart Opera.

**Apple Safari**
- If using Safari version 7 or later, TLS 1.2 is automatically supported.