TLS 1.2 Security Update for Accessing MPUC CMS

What is TLS?

TLS stands for "Transport Layer Security." It is a protocol that provides privacy and data integrity between two communicating applications and is the most widely deployed security protocol used today. TLS is used for web browsers and other applications that require data to be securely exchanged over a network and ensures that a connection to a remote endpoint is the intended endpoint through encryption and endpoint identity verification. There are known vulnerabilities associated with SSL 3.0/TLS 1.0 and 1.1 which allow adversaries to monitor/intercept traffic and decrypt secure transmissions. Updating to TLS 1.2 provides an enhanced level of encryption to protect our network.

How can I avoid a disruption?

Please note that we will be removing support for TLS 1.0 and 1.1 on **July 19, 2018**. If you continue to use an outdated browser you will not be able to connect to our website.

You will need to transition to a browser that supports TLS 1.2. If you are using an older browser, this new technology may be unavailable or may be disabled by default.

Please see the tables below for browser information.

Microsoft Internet Explorer (IE)

Desktop and mobile IE version 11	Compatible with TLS 1.2 or higher by default. If an error message displays and states, "Stronger security is required", then turn off the TLS 1.0 setting in the **Internet Options | Advanced Settings** list.
Desktop IE versions 8, 9, and 10	Compatible only when running Windows 7 or higher, but not by default. Windows Vista, XP and earlier versions are incompatible and cannot be configured to support TLS 1.1 or TLS 1.2.
Desktop IE versions 7 and below	Not compatible with TLS 1.2 or higher encryption.
Mobile IE versions 10 and below	Not compatible with TLS 1.2 or higher encryption.
Microsoft Edge	Compatible with TLS 1.2 or higher by default.

Mozilla Firefox - Compatible with the most versions, regardless of operating system.

Firefox 27 and higher	Compatible with TLS 1.2 or higher by default.
Firefox 23 to 26	Compatible, but not by default. Use about:config to enable TLS 1.2 by updating the security.tls.version.max config value to 3 for TLS 1.2.
Firefox 22 and below	Not compatible with TLS 1.2 or higher encryption.

Google Chrome - Compatible with the most recent version, regardless of operating system.

Google Chrome 38 and higher	Compatible with TLS 1.2 or higher by default.
Google Chrome 22 to 37	Compatible when running on Windows XP SP3, Vista, or newer (desktop), OS X 10.6 (Snow Leopard) or newer (desktop), or Android 2.3 (Gingerbread) or newer (mobile).
Google Chrome 21 and below	Not compatible with TLS 1.2 or higher

Opera

Opera 17 and higher	Compatible with TLS 1.2 or higher by default.
Opera 14 to 16	Not compatible with TLS 1.2 or higher encryption.
Opera 10 to 12	Compatible, but not by default.
Opera 9 and below	Not compatible with TLS 1.2 or higher encryption.

Google Android OS Browser

Android 5.0 (Lollipop) and higher	Compatible with TLS 1.2 or higher by default.
Android 4.4 (KitKat) to 4.4.4	May be compatible with TLS 1.1 or higher. Some devices with Android 4.4.x may not support TLS 1.1 or higher.
Android 4.3 (Jelly Bean) and below	Not compatible with TLS 1.2 or higher encryption.

Apple Safari

Desktop Safari versions 7 and higher for OS X 10.9 (Mavericks) and higher	Compatible with TLS 1.2 or higher by default.
Desktop Safari versions 6 and below for OS X 10.8 (Mountain Lion) and below	Not compatible with TLS 1.2 or higher encryption.
Mobile Safari versions 5 and higher for iOS 5 and higher	Compatible with TLS 1.2 or higher by default.
Mobile Safari for iOS 4 and below	Not compatible with TLS 1.2 or higher encryption.

How to Guide: Enabling SSL Version TLS 1.2

Microsoft Internet Explorer (IE)

1. Open Internet Explorer.
2. Click **Alt-T** and select **Internet Options**.
3. Select the **Advanced** tab.
4. In the "Security" section, locate and check Use **TLS 1.2**

Firefox

1. Open Firefox.
2. Type in "about:config" in the URL bar and press **Enter**.
3. Scroll down to "security.tls.version.max" and press **Enter**.
4. Set the value to **3**.
5. Click OK.

Google Chrome

1. Open Google Chrome.
2. Click **Alt-F** and select **Settings**.
3. Scroll down and select **Show advanced settings...**
4. In the Network section, click **Change proxy settings...**
5. Select the "Advanced" tab.
6. In the "Security" section, locate and check **Use TLS 1.2**.
7. Click OK.

Opera

1. Open Opera.
2. Click **Ctrl+F12**.
3. Click **Security**.
4. Click **Security Protocols...**
5. Check **Enable TLS 1.2**.
6. Click **OK**.
7. Click **OK** again.

Safari

1. There are no options for enabling SSL protocols. TLS 1.2 are automatically enabled, if you are using Safari version 7 or greater.