TLS 1.0 Security Announcement Date: May 2016

In order to maintain PCI compliancy, the Transport Layer Security (TLS) level being used to process payments must be upgraded. PSN carries the burden of maintaining PCI compliancy for the processing of your electronic payments. In order to maintain PCI compliant status, PSN must disable TLS 1.0 as a security method being used for payment processing by June 30, 2016. Going forward PSN will process transactions using TLS 1.2.

This document details the steps required for the TLS change to prevent any interruption in the ability to accept payments.

A server side setting is required to accommodate all payments entered/processed by the utility.

Payments made by customers via ***Utilit-e Online*** & MCA may require a browser setting change depending on the user's (utility customer or utility staff) browser and version.

Payments made via *Utilit-e Connect*:

Input Payments, Payment Options and Scheduled Payments

- ***Utilit-e Central*** **Hosted Solutions**
  - For utilities hosted in ***Utilit-e Central***, PCS will make the necessary server side changes.
  - You do not have to do anything for payments made via ***Utilit-e Connect***.

- **In-house Solutions**
  - For utilities with PCS applications on a server within the utility, please see the instructions in the Server Side Instructions area of this document.

Payments made via *Utilit-e Online*:

Users (customers or staff) may experience problems making payments if they do not have TLS1.2 enabled in their browser settings.

- The newest versions of Google Chrome, Mozilla Firefox, Internet Explorer and Apple Safari support TLS 1.1 and TLS 1.2 by default.
- Users of older versions of browsers may need to enable TLS 1.1 and 1.2 on their browsers to make a payment if it is not already enabled.

PCS Confidential

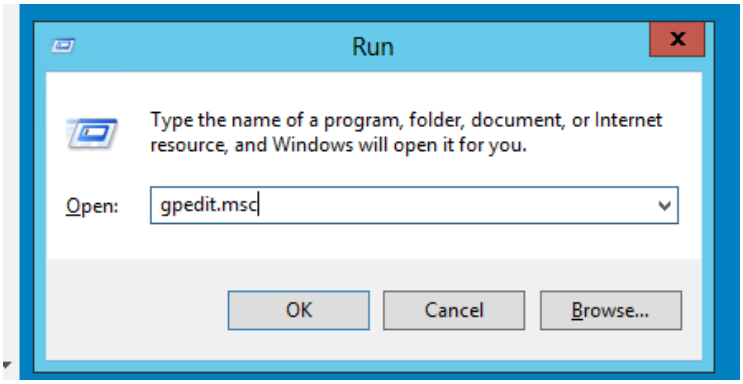
Server Side Instructions

This needs to be done on Windows Server 2012 (Non-R2) Application servers only. Other versions of Windows Server (2008 R2 and 2012 R2) already have this setting by default. PCS recommends confirming the default setting is still in place allowing "Use TLS 1.0, TLS 1.1 and TLS 1.2". The steps for checking this setting for 2008 R2 and 2012 R2 are similar to those described below for Windows Server 2012 (Non-R2).

Database servers do not need this setting.

Windows Server 2012 (Non-R2)

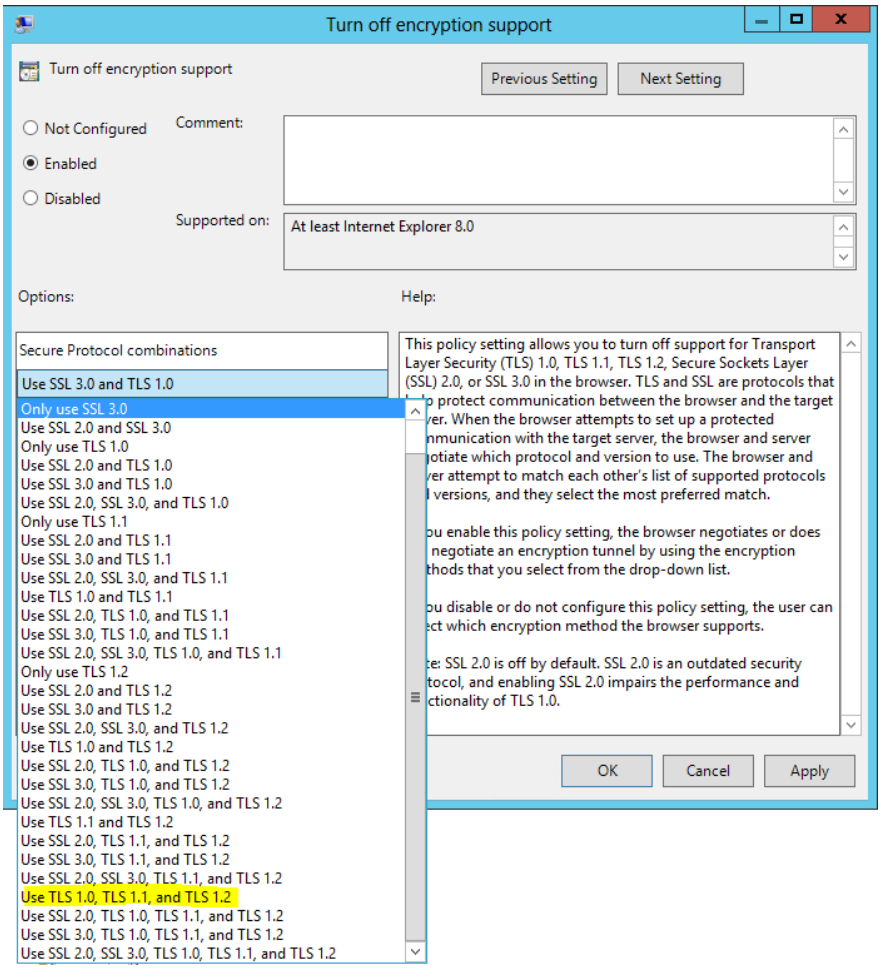
Open up a Run prompt (Windows Key + R) and type gpedit.msc



Navigate to Computer Configuration > Administrative Templates > Windows Components > Internet Explorer > Internet Control Panel > Advanced Page > Turn Off Encryption Support

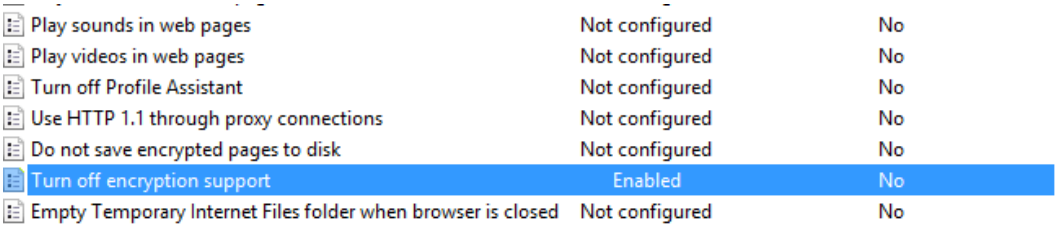
PCS Confidential

The following screen will display:



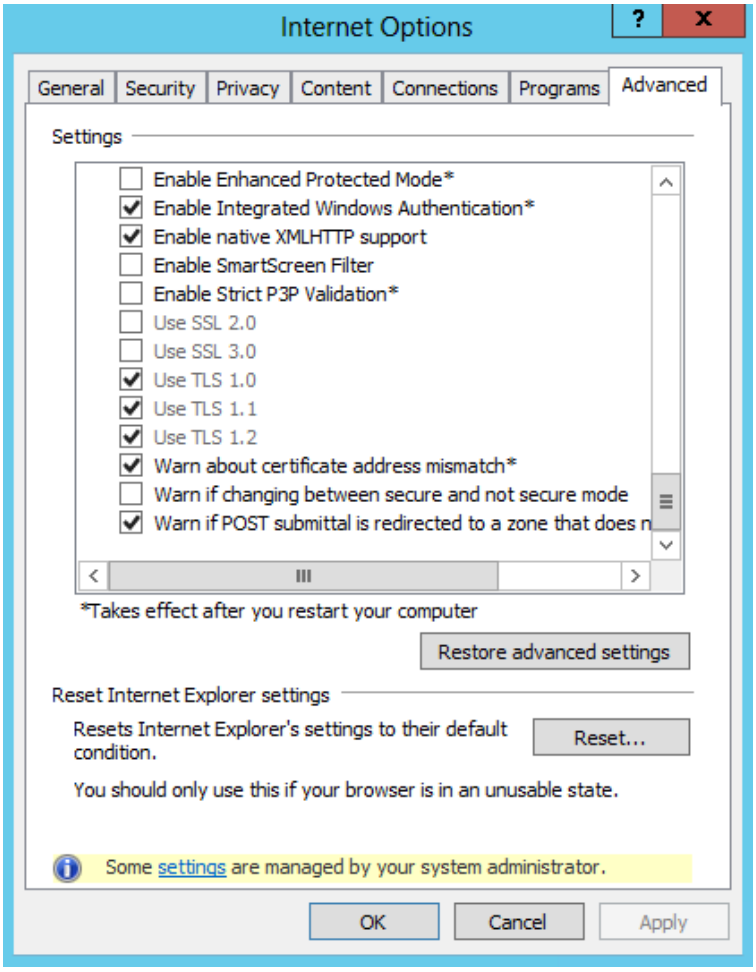
Change the setting to “Enabled”. There will be many options in the drop down box. PCS recommends the highlighted option of “Use TLS 1.0, TLS 1.1, and TLS 1.2” to turn off SSL 2.0 and SSL 3.0, but leave TLS 1.0 on while turning on TLS 1.1 and TLS 1.2. This will allow access to some legacy websites while still using the newer versions of TLS for more secure websites like PSN and online banking.

Click OK and the Policy will show as Enabled.



Close the GPO editor, the settings save automatically.

Check that the policy was applied by going to Internet Explorer > Tools > Internet Options > Advanced Tab. All three TLS settings should be checked like shown below.



PCS recommends doing this locally on the server that needs the setting, but this can be done from a domain controller and applied to the whole domain or a group of servers if that is preferred.

PCS Confidential

PC Side Instructions

The newest versions of Google Chrome, Mozilla Firefox, Internet Explorer, Microsoft Edge and Apple Safari support TLS 1.1 and TLS 1.2 by default. Older versions of browsers, however, may need to have TLS 1.1 and TLS 1.2 enabled. If they are not enabled, users will not be able to make payments via ***Utilit-e Online***. This applies to both customers and utility staff. For utility staff this is specifically, referencing using the browser on the individual's PC not the browser from within the remote desktop (RDP) session.

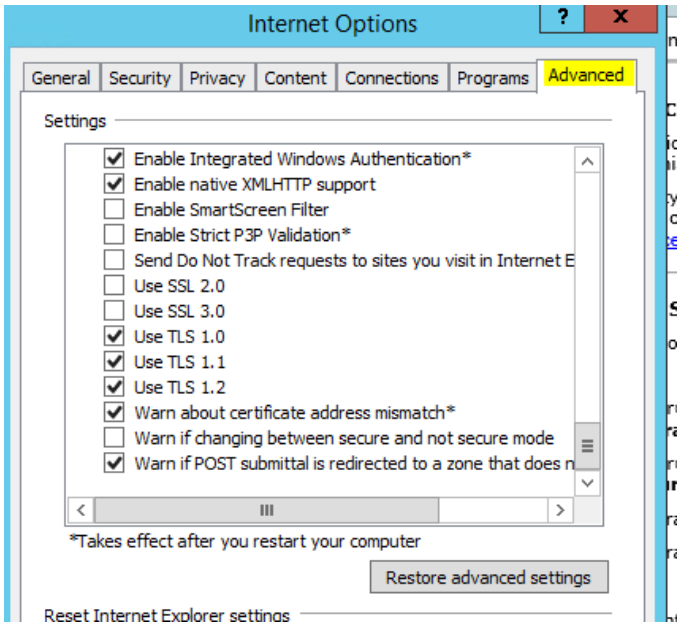
Following are instructions for the various browsers to check and/or change these settings as needed.

Internet Explorer

If you are using Internet Explorer version 10 or older. Follow these steps to enable TLS 1.1 and TLS 1.2:

Click the Settings Gear in the top right corner

Click Advanced and click the check boxes for TLS 1.1 and TLS 1.2

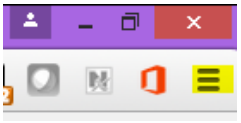


Click OK and restart Internet Explorer

PCS Confidential

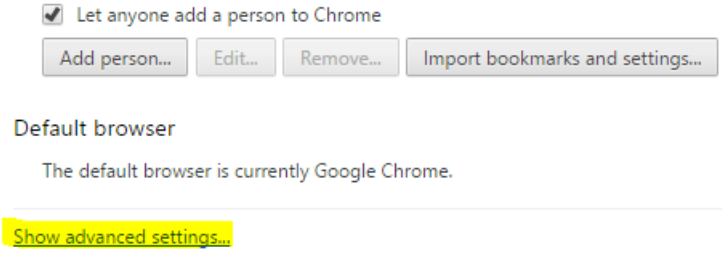
Google Chrome

If you are using Google Chrome. Follow these steps to enable TLS 1.1 and TLS 1.2:
Click the menu bar in the top right corner

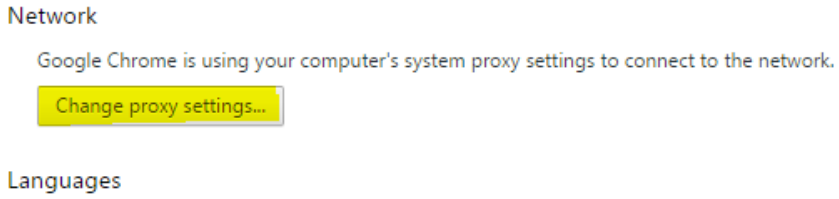


Choose Settings from the menu

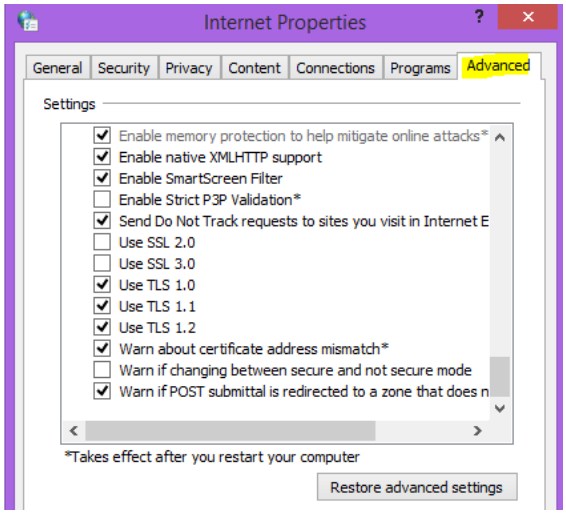
Click Show advanced settings…. At the bottom of the page



Scroll down to the Network section and click Change proxy settings…



Click on the Advanced tab, scroll all the way down and make sure that TLS 1.1 and TLS 1.2 are checked



PCS Confidential