Australian Government
Department of Education and Training

HEIMS Applications Upgrade

The department undertook security risk assessment of all applications its hosts and its findings recommended the use of TLS 1.2 protocol to enhance the security of information communicated over the Internet. This change is necessary due to the potential for future protocol downgrade attacks and other TLS 1.0/1.1 vulnerabilities not specific to department's implementation.

As a result, from 1 October 2018 the department will disable SSL 2.0/ SSL 3.0, TLS 1.0/1.1 and use TLS 1.2 instead for all HEIMS web applications and web services.

Web Browsers – HEIMS Online and HEIMS Admin

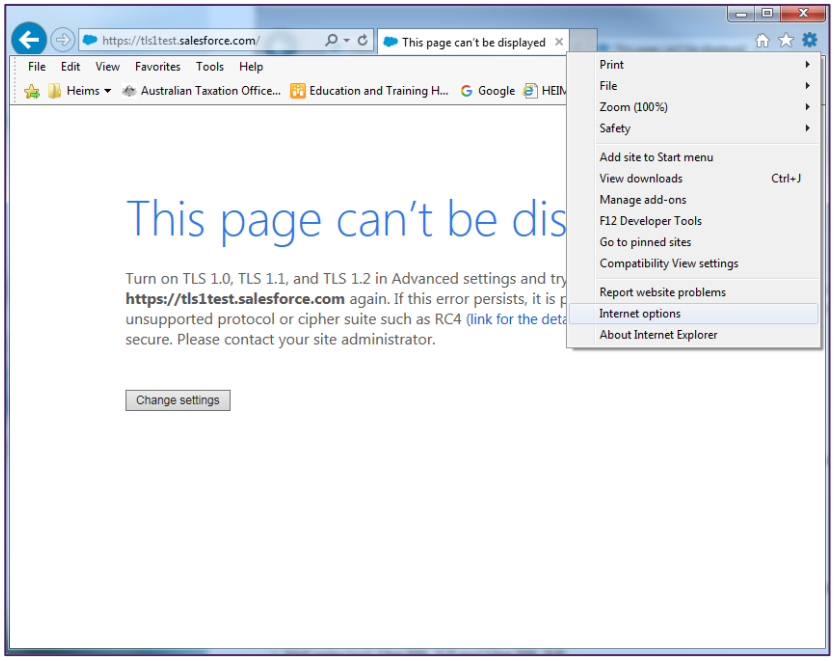
TLS 1.2 compliant browser is needed to access HEIMS Online / HEIMS Admin from 1 October 2018. This change means you won't be able to access HEIMS Web applications using **Internet Explorer 9 or 10** on **Windows 8 and 7** without making changes to your browser settings. The following workaround could be considered as a guide while using Internet Explorer 9 or 10.

This table below shows which versions of Internet Explorer have TLS 1.2 enabled by default, the versions you need to enable TLS 1.2 manually, and versions that are not supported:

Internet Explorer version	Windows 8.1 and newer	Windows 8 and 7	Windows Vista, XP and older
11	Enabled by default	Enabled by default	Enabled by default
10, 9	Enabled by default	You need to enable TLS 1.2 manually	Not supported

How to enable TLS 1.2 manually?

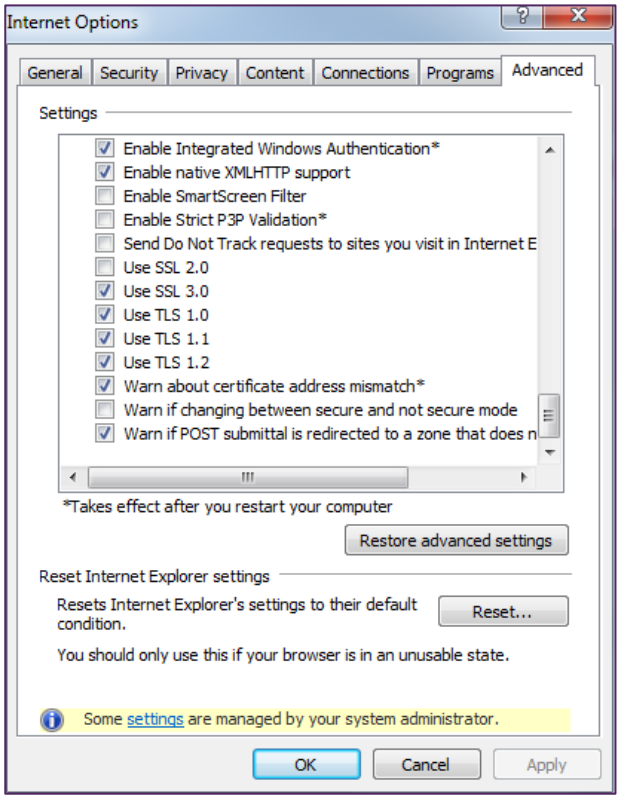
1 Open the Tools menu (click the cog icon near the top-right of Internet Explorer) and choose Internet options:



2 Select the Advanced tab.

3 Scroll down to the Security section at the bottom of the settings list.

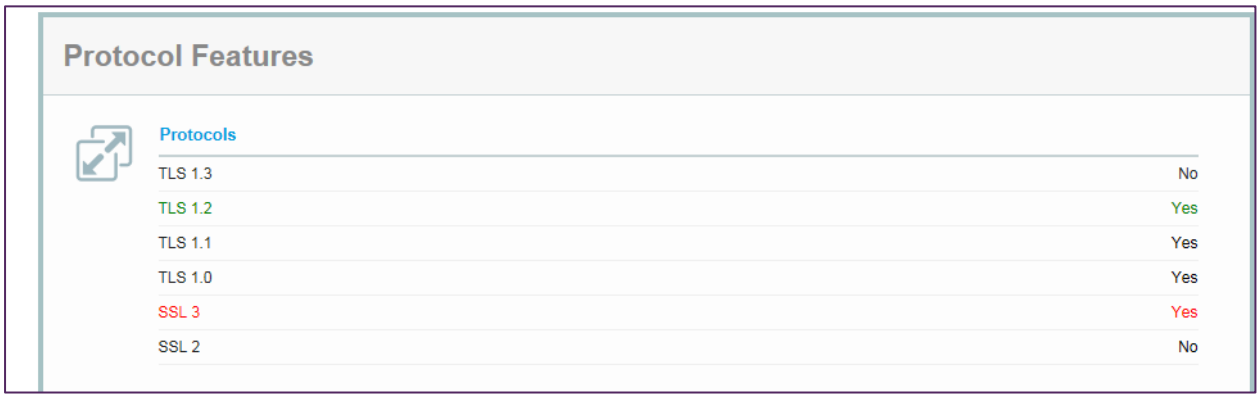
4 Select the checkbox TLS 1.2



5 Click Apply.

6 Click OK.

You can confirm the TLS compliance of the browser by accessing below link as a guide:
https://www.ssllabs.com/ssltest/viewMyClient.html



HEIMS Web Services (CHESSN, Application and Offers and Scholarships)

Providers consuming HEIMS Web Services should ensure that their client application supports TLS 1.2 and Server Name Identification (SNI) while communicating with HEIMS Web Services as of 1 October 2018. Since each provider's client application implementation may vary we recommend you contact your IT support team to ensure TLS 1.2 and SNI compliance of client application. You may use SSL Labs and DigiCert SSL Installation Diagnostic tool to check the certificates and ciphers used.

You may refer to below links as a guide for TLS 1.2 compliance.

https://blogs.msdn.microsoft.com/bing_ads_api/2018/02/02/mandatory-upgrade-required-to-tls1-2/

https://www.digicert.com/help/

https://www.ssllabs.com/ssltest/

HEPCAT

TLS 1.2 support will be enabled in HEPCAT as part of the next release scheduled in July 2018.