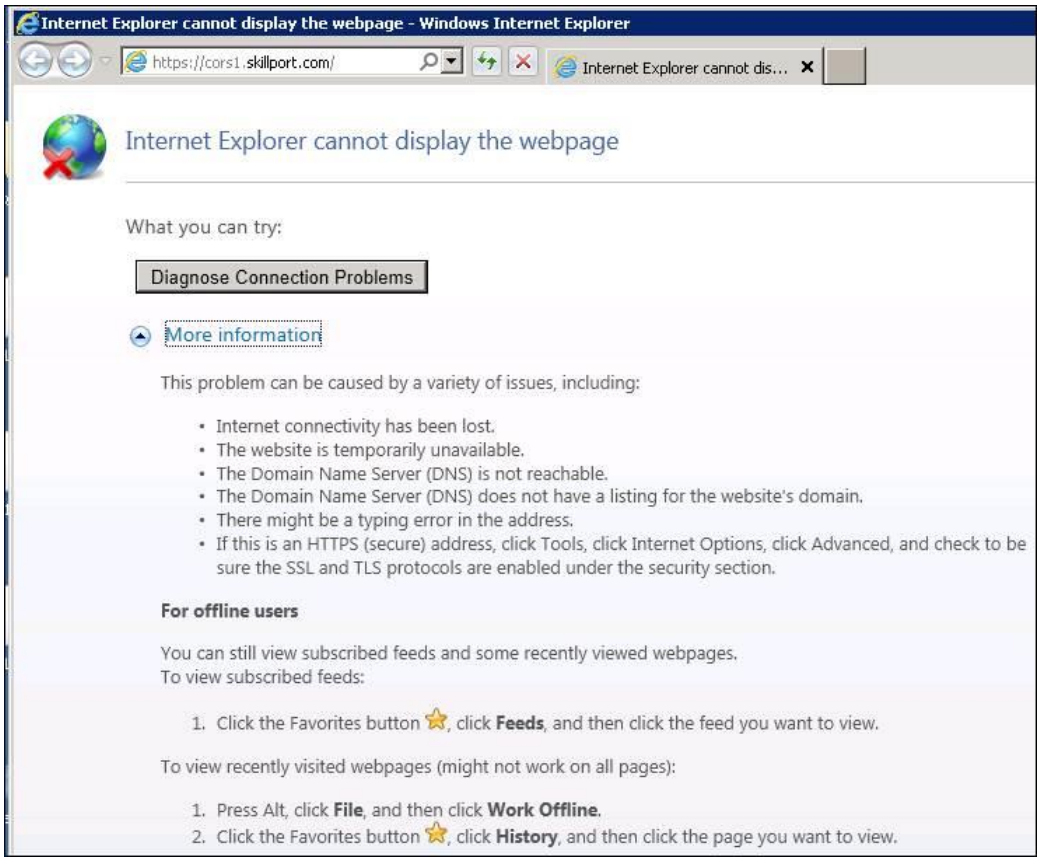
TLS 1.2 Enablement Frequently Asked Questions

Click for answers to specific questions regarding:

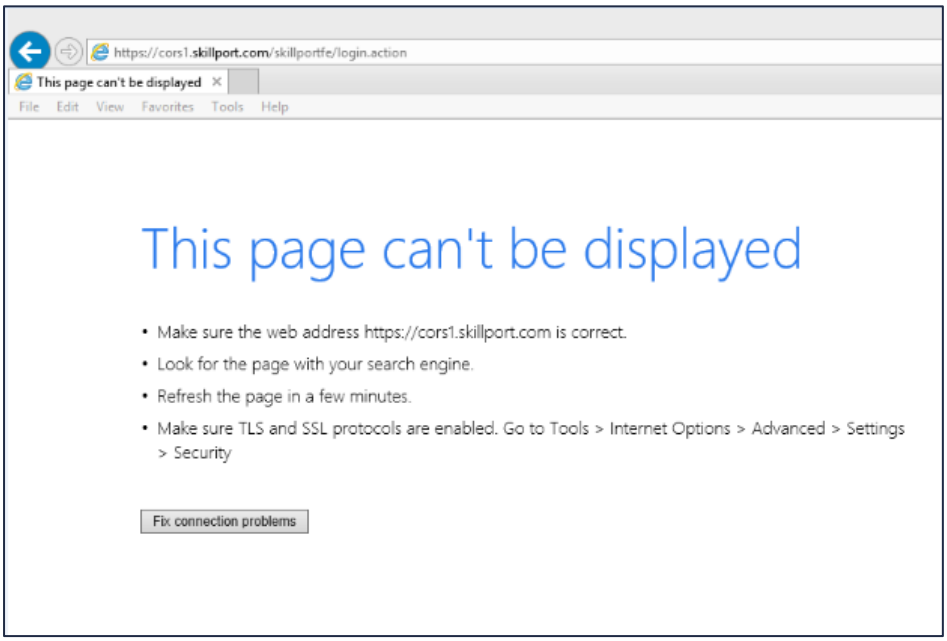
If your question is not answered below, please contact your Skillsoft Account team or Support@skillsoft.com with additional questions.

Question	Answer
Background	
What is TLS?	Transport Layer Security (TLS) is a cryptographic protocol providing communications security over computer networks such as those used by browsers and applications connecting to hosted cloud services. TLS 1.2 is the latest supported version of the protocol.
Why is Skillsoft making this change to support only TLS 1.2 or later?	Skillsoft implemented mandatory HTTPS in June 2017, and currently supports earlier TLS versions. Security threats have become more serious and more frequent, and TLS 1.0 and 1.1 have been demonstrated to be vulnerable to attack. Disabling earlier versions of TLS and supporting only TLS 1.2 is an industry practice that is strongly recommended, especially when the data transmitted is considered sensitive.
What is Skillsoft actually doing?	Skillsoft will disable TLS 1.0 and 1.1 on all Skillsoft cloud services and, will only accept connections using TLS 1.2.
Impact, Date, & Duration	
Will the change affect me?	You may be impacted if you use any of Skillsoft's APIs (SOAP-based OLSA or the legacy BCS), and your implementation does not support TLS 1.2.

When is the change happening?	Skillsoft will make this change to all cloud services on the morning of June 1, 2018.
Will this change require a service outage?	No. There will be no outage.
Will any URLs change?	No, this will not require any changes to the URLs you are using.
Will my users see any differences?	No, this move will be transparent, so long as users are using a browser that supports TLS 1.2. However, browsers which do not support TLS 1.2 will be unable to connect to any Skillsoft hosted services. Skillsoft supports the following browsers, which all support TLS 1.2: • Microsoft Edge v14+ (Windows 10 only) • Microsoft IE v11 (Windows 7, 8.1, 10) • Google Chrome v63+ (Windows 7, 8.1, 10) • Mozilla Firefox v52+ (Windows 7, 8.1, 10) • Apple Safari v10.1+ (macOS only)
What will users see if they are using a browser that does not support TLS 1.2?	Internet Explorer 8 and 9 will display the following message:  If the user clicks to show More information, they will see the following:



Internet Explorer 10 will display the following message:



Do I need to do anything?	We recommend that you notify your IT department to make sure that we can answer any additional questions they may have.

	Any other actions will depend on how you access Skillsoft services, and functionality you have. If you use any of the following you may need to take action: • Use Skillsoft Hosted Content Server (OLSA Server) with an LMS • Use Skillsoft Web Services API (OLSA Web Services) • Use Skillsoft Legacy API (BCS)
Impact on Skillsoft Hosted Content Server (OLSA Server) with an LMS	
Do I need to do anything to reload all my courses?	No, the URLs will not change and so the courses will not need to be updated.
My LMS uses the OLSA Automation Features. Do I need to change anything?	You should confirm with your LMS vendor that your OLSA Automation Feature is capable of supporting TLS 1.2 connections. For more details see the section on **Skillsoft Web Services API (OLSA Web Services)**
Impact on Skillsoft Web Services API (OLSA Web Services)	
Do I need to do anything?	You should confirm that your implementation of the SOAP-based OLSA Web Services is capable of supporting TLS 1.2 connections. As of June 1st, the OLSA Web Services EndPoint will reject any connections that do not use TLS 1.2 and the automation will not work.
Do I need to wait to make these changes?	No, you should start checking your applications can connect using TLS 1.2.
Can you help troubleshoot my application?	Skillsoft cannot provide individual guidance on exactly what changes may be needed to your application. However, we do have test sites available that can be used to test TLS 1.2 communication.

	See the list of resources at end of this document for some reference links.
Is there a way I can test this before the change is implemented?	Yes. Skillsoft has a number of test sites that are configured to require TLS 1.2. Please contact support@skillsoft.com for information on how to access a test site.
Impact on Skillsoft Legacy API (BCS)	
Do I need to do anything?	You should confirm that your implementation of the legacy BCS API is capable of supporting TLS 1.2 connections. As of June 1st, the BCS API will reject any connections that do not use TLS 1.2 and the automation will not work.
Do I need to wait to make these changes?	No, you should start checking your applications can connect using TLS 1.2.
Can you help troubleshoot my application?	Skillsoft cannot provide individual guidance on exactly what changes may be needed to your application. However, we do have test sites available that can be used to test TLS 1.2 communication. See the list of useful resources at end of this document for some reference links.
Is there a way I can test this before the change is implemented?	Yes. Skillsoft has a number of test sites that are configured to require TLS 1.2. Please contact support@skillsoft.com for information on how to access a test site.

Useful Developer References for Enabling TLS

Applications using Microsoft .NET technologies	To enable TLS 1.2, you must install the **.NET framework 4.5 or later**. The following Microsoft article explains how to configure the protocols and ciphers enabled on the servers, and provides details on using NetMon to diagnose connection issues. https://blogs.msdn.microsoft.com/friis/2017/10/09/troubleshooting-tls-ssl-scenario-2/ The patch and registry change documented here Microsoft Security Advisory 2960358 https://docs.microsoft.com/en-us/security-updates/SecurityAdvisories/2015/2960358 will enable all .NET applications running on this machine to use TLS 1.2 If the developer wishes to enable this functionality via a code change, they can add the following line of code (C#) before any WebRequests are made. `System.Net.ServicePointManager.SecurityProtocol = System.Net.SecurityProtocolType.Tls12;`
Applications using Java	To enable TLS 1.2, you must use a **JDK 8 releases, or Java 7 update 95 (January 2016), or Java 6 update 121 (July 2016)** The following Oracle article provides some good background on the support for TLS https://blogs.oracle.com/java-platform-group/diagnosing-tls,-ssl,-and-https Some of the key points: • JDK8 – TLSv1.2 is default • JDK7 – TLSv1.2 must be explicitly enabled

	• JDK6 – TLSv1.2 must be explicitly enabled • JDK6/JDK7 – Can be enabled with Java System Properties statically on command line (-`Dhttps.protocols="TLSv1.2" -Djdk.tls.client.protocols="TLSv1.2"`) • JDK6/JDK7 – Can be enabled by setting above Java System Properties via code
Applications using Ruby	To enable TLSv1.2, you must use **Ruby 2.0.0 or later and OpenSSL 1.0.1c or later** are required: • Ruby 2.0.0 or later is required to use TLSv1.2 from the system-supplied OpenSSL. • TLSv1.2 requires OpenSSL 1.0.1c or later. Please refer https://github.com/ruby/openssl for more information
Applications using Python	To enable TLSv1.2, you must use **OpenSSL 1.0.1c or later**: • Python uses the system-supplied OpenSSL. • TLSv1.2 requires OpenSSL 1.0.1c or later. Please refer https://docs.python.org/2/library/ssl.html for more information
Applications using PHP with the cURL PHP extension	To enable TLSv1.2, you must use **PHP v5.3.0, and with cURL 7.3.4** Within your code you should set the cURL SSLVERSION http://php.net/manual/en/function.curl-setopt.php `$ch = curl_init();`

	`curl_setopt($ch, CURLOPT_URL, "{URLTOOPEN}");` `curl_setopt($ch, CURLOPT_SSLVERSION, 6);`
Applications using PHP stream_socket_client()	To enable TLSv1.2, you must use **PHP v5.6.0** http://php.net/manual/en/migration56.openssl.php#migration56.openssl.crypto-method

If you wish to confirm your environment is able to connect using TLS 1.2, you can use the open source API available here: https://www.howsmyssl.com/s/api.html.

This API returns details of how your application negotiated a connection to the server, and returns a JSON object. You should verify that the "`tls_version`" value is `"TLS 1.2".`