SECURITY
WITH
PLYMOUTH
UNIVERSITY

Technology & Information Services

SEC-GDL-001 – Secure Online Browsing Guidelines

Author:	Paul Ferrier
Date:	21/04/2017
Document Security Level:	**PUBLIC**
Document Version:	0.91
Document Ref:	SEC-GDL-001
Document Link:	
Review Date:	April 2018

Document Control							
Version	**Author**	**Position**	**Details**	**Date/Time**	**Approved by**	**Position**	**Date/Time**
0.9	Paul Ferrier	Enterprise Security Architect	Created the document	21/04/2017 11:40			
0.91	PF	ESA	Updated following comments	04/05/2017 16:35			

Table of Contents

SEC-GDL-001 – Secure Online Browsing Guidelines

Purpose

All information both at home and in the workplace, has some form of value and therefore needs to be protected against unauthorised exposure and disclosure.

Consider online banking, you would want to ensure that the data sent between your device and the bank to be secure and not susceptible to interception.

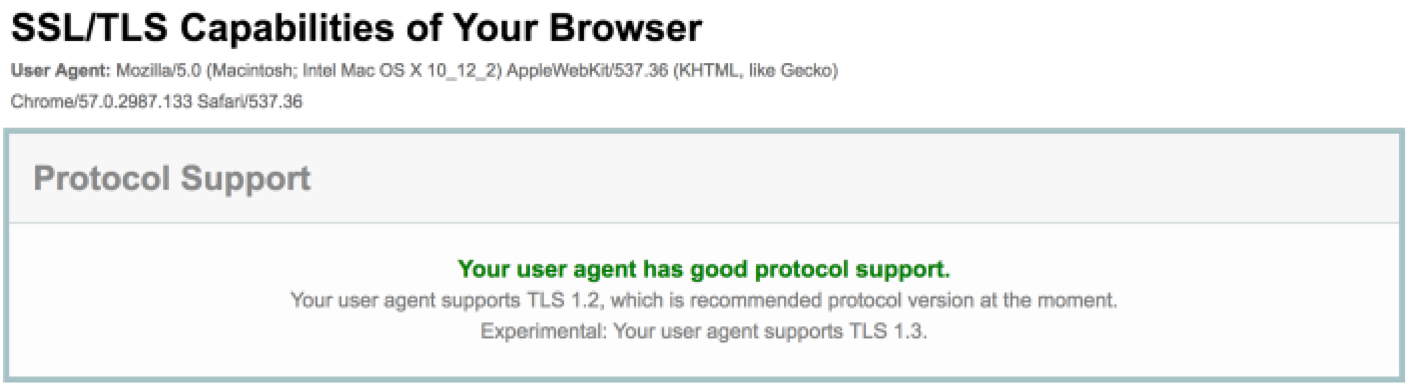
Over time, vulnerabilities in communication encryption methods are discovered and need to be updated or retired to ensure that the information is kept secure.

Definitions

Cipher	An algorithm for performing encryption or decryption
Encryption	A method for disguising (or enciphering) information with a series of instructions
Protocol	Describes how the algorithms should be used to encrypt information
SSL	(Security Sockets Layers) is a standard security technology for establishing an encrypted link between a web server (covers web browsing, email, instant messaging and Voice over IP) and a client browser
TLS	(Transmission Layer Security) is the successor to SSL and performs the same functionality with more secure methods
Vulnerability	Is a weakness which allows an attacker to reduce a systems' information assurance

How can I find out what my Internet browser supports?

There is a site (https://www.ssllabs.com/ssltest/viewMyClient.html) that offers a free test of your Internet browsers' capabilities in terms of secure communications. It also provides details as to whether the software is susceptible to known vulnerabilities.



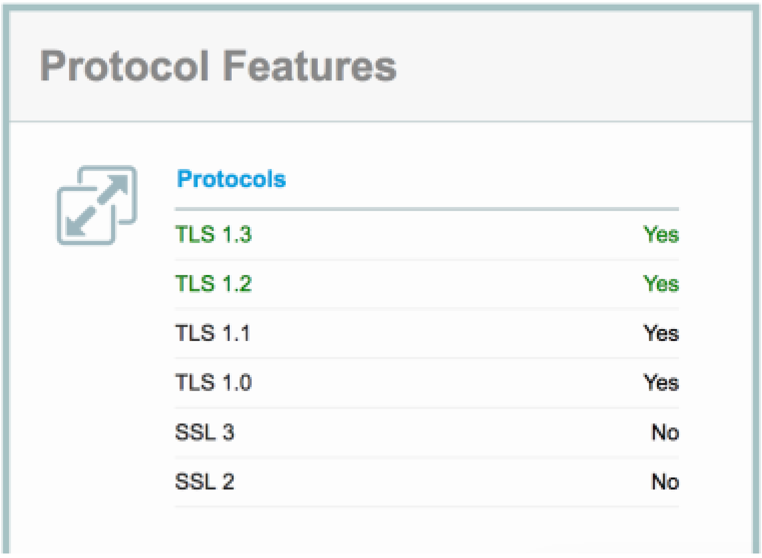
SSL/TLS Capabilities of Your Browser

User Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_2) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/57.0.2987.133 Safari/537.36

Protocol Support

Your user agent has good protocol support.
Your user agent supports TLS 1.2, which is recommended protocol version at the moment.
Experimental: Your user agent supports TLS 1.3.

Further down the page, it lists the protocols (in Protocol Features) that are available to communicate with the web servers that you communicate with.

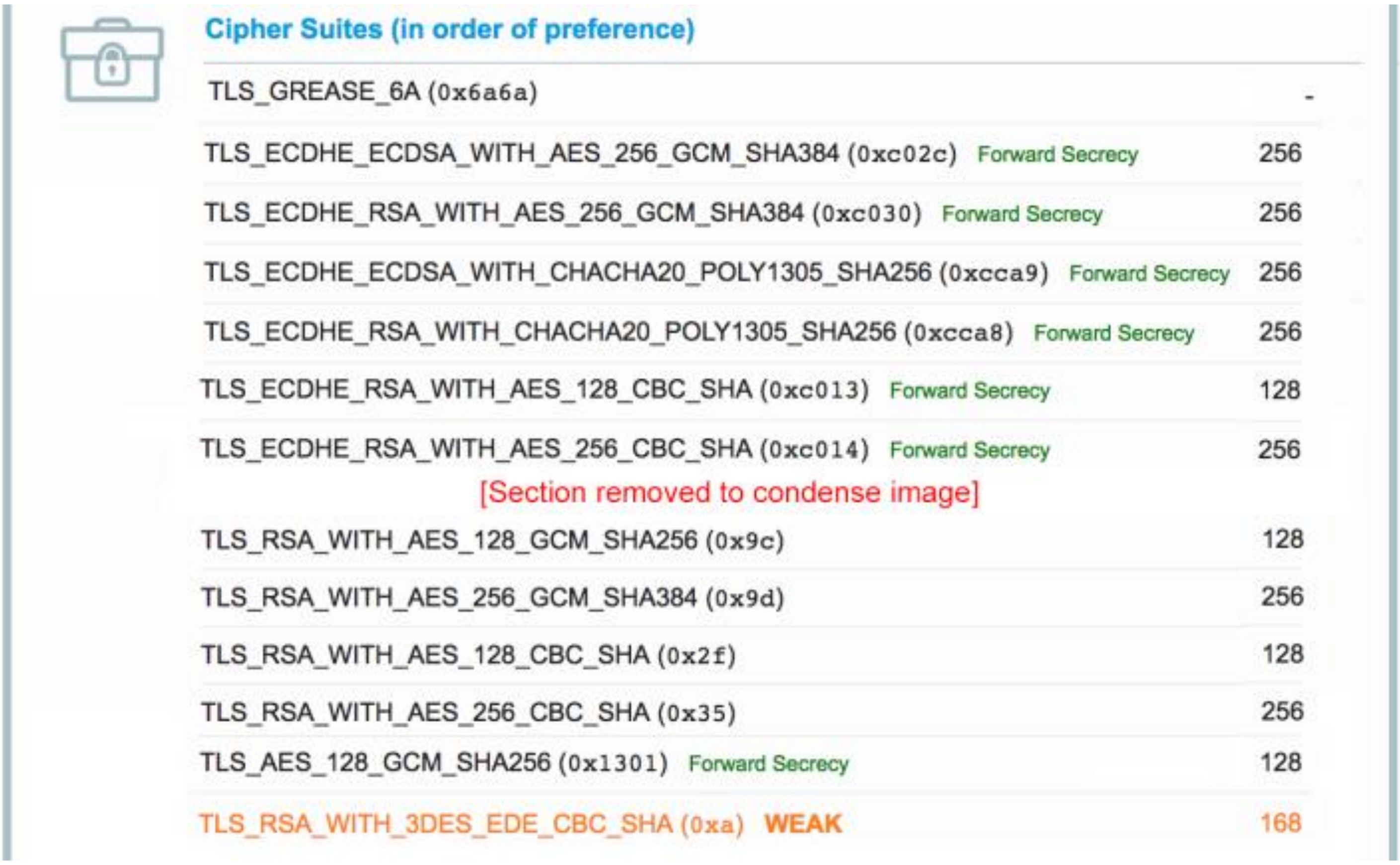


Protocol Features

Protocols	
TLS 1.3	Yes
TLS 1.2	Yes
TLS 1.1	Yes
TLS 1.0	Yes
SSL 3	No
SSL 2	No

This displays in green the secure protocols that are available for use, black are available for use, and red display a protocol that is insecure.

As well as protocols, there is also a list of ciphers, similarly to the protocols they are colour coded for ease of identification. The top cipher suite in the list is solely for use with TLS 1.3 protocol, this can be easily identified by having no value on the right-hand side (that denotes the length of the encryption key) as random lengths are introduced for added security.



Cipher Suites (in order of preference)		
TLS_GREASE_6A (0x6a6a)		-
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)	Forward Secrecy	256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	Forward Secrecy	256
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9)	Forward Secrecy	256
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8)	Forward Secrecy	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	Forward Secrecy	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	Forward Secrecy	256
[Section removed to condense image]		
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c)		128
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d)		256
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)		128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)		256
TLS_AES_128_GCM_SHA256 (0x1301)	Forward Secrecy	128
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)	WEAK	168

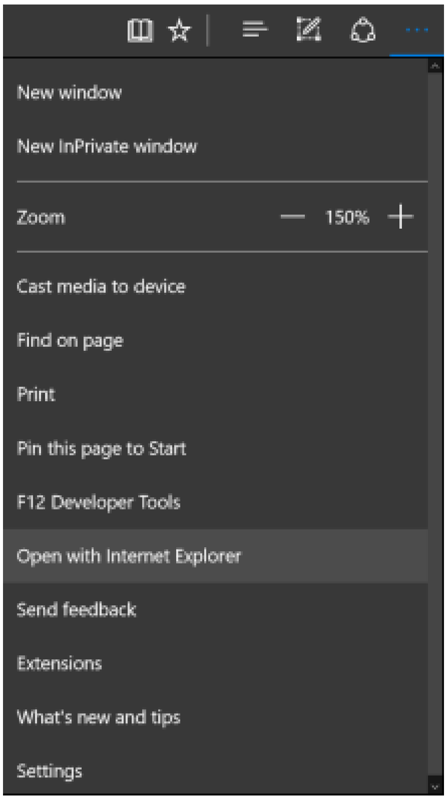
How can I disable insecure or activate secure protocols?

The heading may be misleading, you are not able to add or remove protocols and ciphers (as they are part of the computers Operating System), however, you can enable or disable them for use.

There are two main options here that either involve changing settings in your Internet browser or make changes to your computers' registry settings.

Microsoft Edge

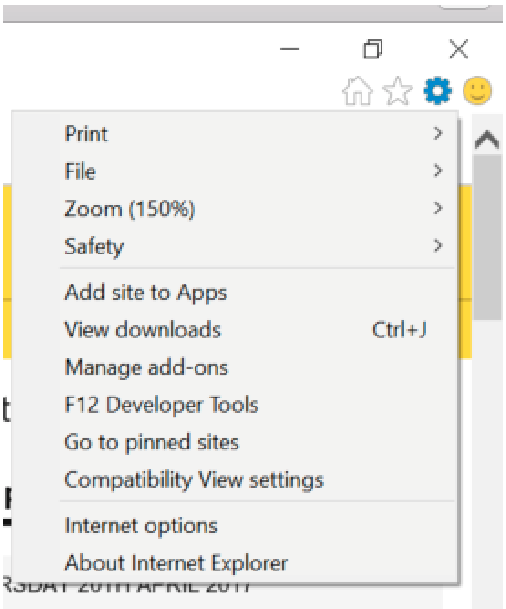
Unfortunately, due to the nature of Microsoft Edge you do not have the ability to change settings in relation to TLS natively in this browser; however, you can open a web page and then select from the three dots on the right hand side Open with Internet Explorer – this will allow you to then follow the steps below in the Internet Explorer section.

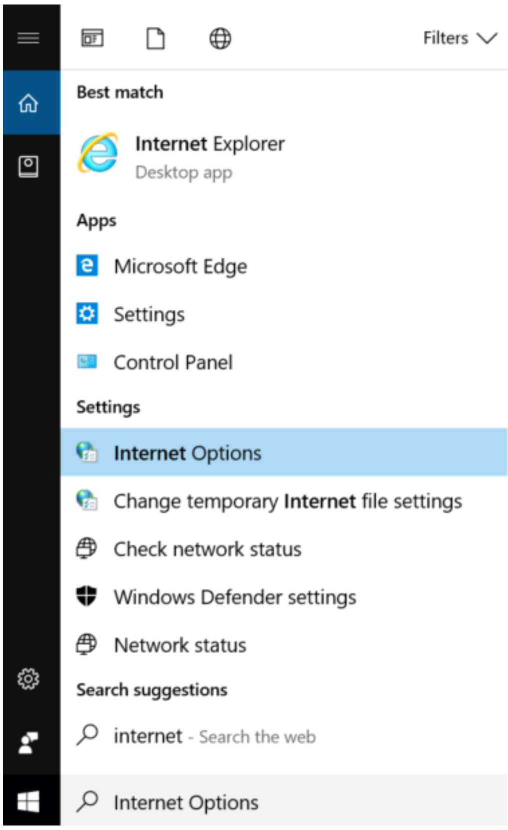


Microsoft Internet Explorer

On a Windows computer, change your Internet browser settings through ***Internet Explorer***

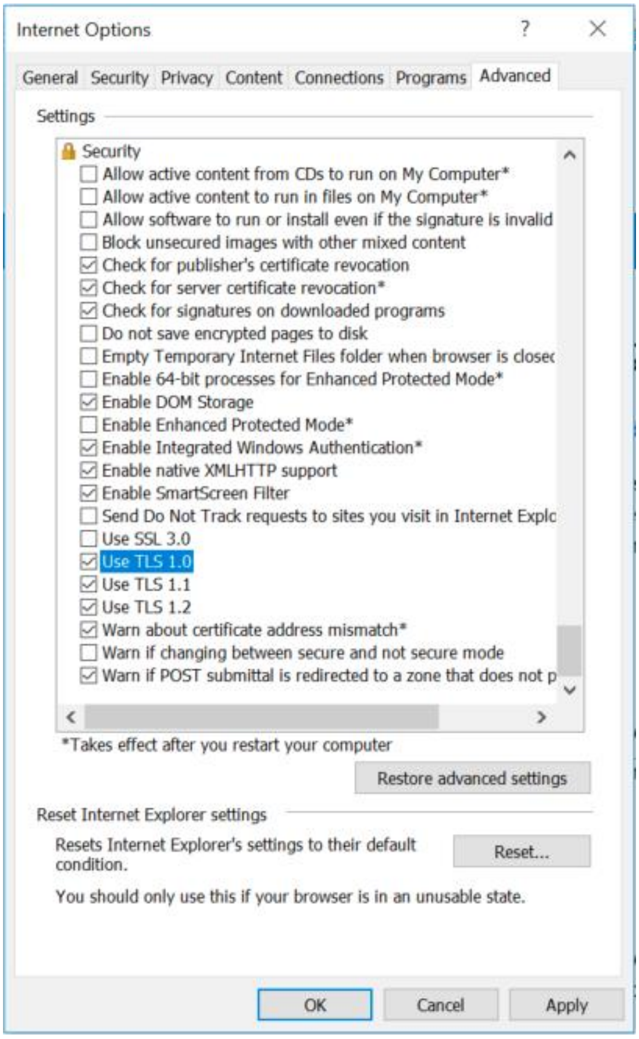
To access the Internet Explorer settings, either in your browser go to the **cogs** on the right-hand side of the window and then select **Internet options**, ***or*** search for **Internet options** in the search bar. Please note the images below will be a little different on Windows 7 and Windows 10, but they are accessed in the same way.





Internet Options

When the Internet Options window is open, navigate to the **Advanced** tab and scroll down to the **Security** section.



Security
- ☐ Allow active content from CDs to run on My Computer*
- ☐ Allow active content to run in files on My Computer*
- ☐ Allow software to run or install even if the signature is invalid
- ☐ Block unsecured images with other mixed content
- ☑ Check for publisher's certificate revocation
- ☑ Check for server certificate revocation*
- ☑ Check for signatures on downloaded programs
- ☐ Do not save encrypted pages to disk
- ☐ Empty Temporary Internet Files folder when browser is closec
- ☐ Enable 64-bit processes for Enhanced Protected Mode*
- ☑ Enable DOM Storage
- ☐ Enable Enhanced Protected Mode*
- ☑ Enable Integrated Windows Authentication*
- ☑ Enable native XMLHTTP support
- ☑ Enable SmartScreen Filter
- ☐ Send Do Not Track requests to sites you visit in Internet Explc
- ☐ Use SSL 3.0
- ☑ Use TLS 1.0
- ☑ Use TLS 1.1
- ☑ Use TLS 1.2
- ☑ Warn about certificate address mismatch*
- ☐ Warn if changing between secure and not secure mode
- ☑ Warn if POST submittal is redirected to a zone that does not p

*Takes effect after you restart your computer

Resets Internet Explorer's settings to their default condition.

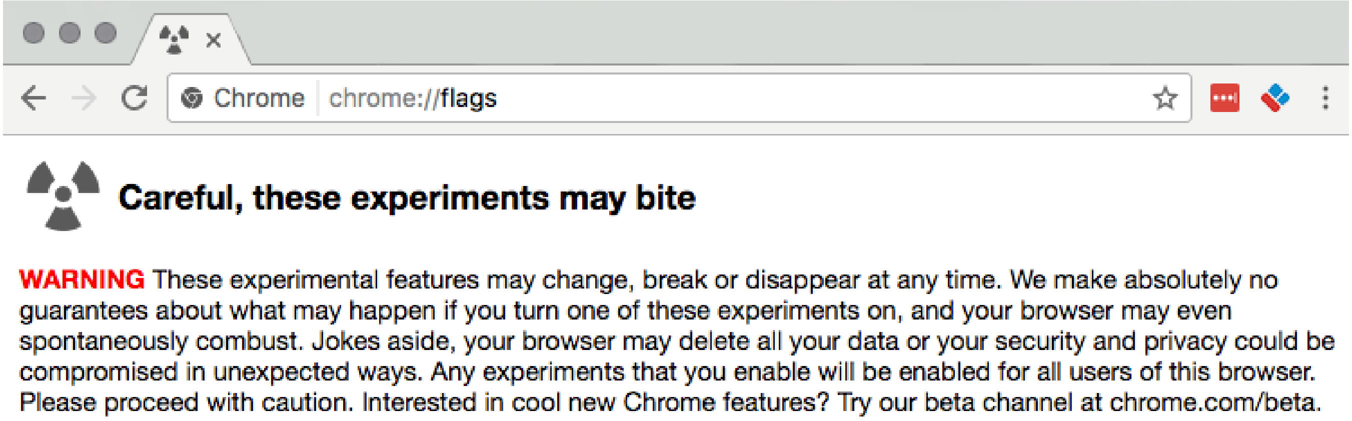
You should only use this if your browser is in an unusable state.

Uncheck the **Use TLS 1.0** and **Use TLS 1.1**. You may need to allow TLS 1.1 if you encounter problems accessing some sites however it is not a long term option that is sustainable, as it will be removed from University services later in 2017.

When you click **Apply** the settings will take effect after next rebooting your computer.

Google Chrome

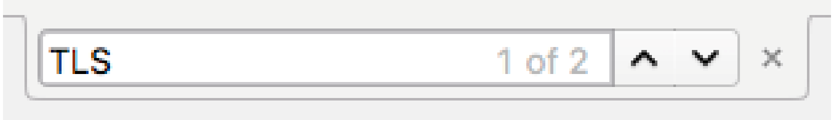
On a computer, change your Internet browser settings through ***Google Chrome***.
To access the Chrome settings, in the address bar type: **chrome://flags** and you will be presented with a warning screen depicted below:



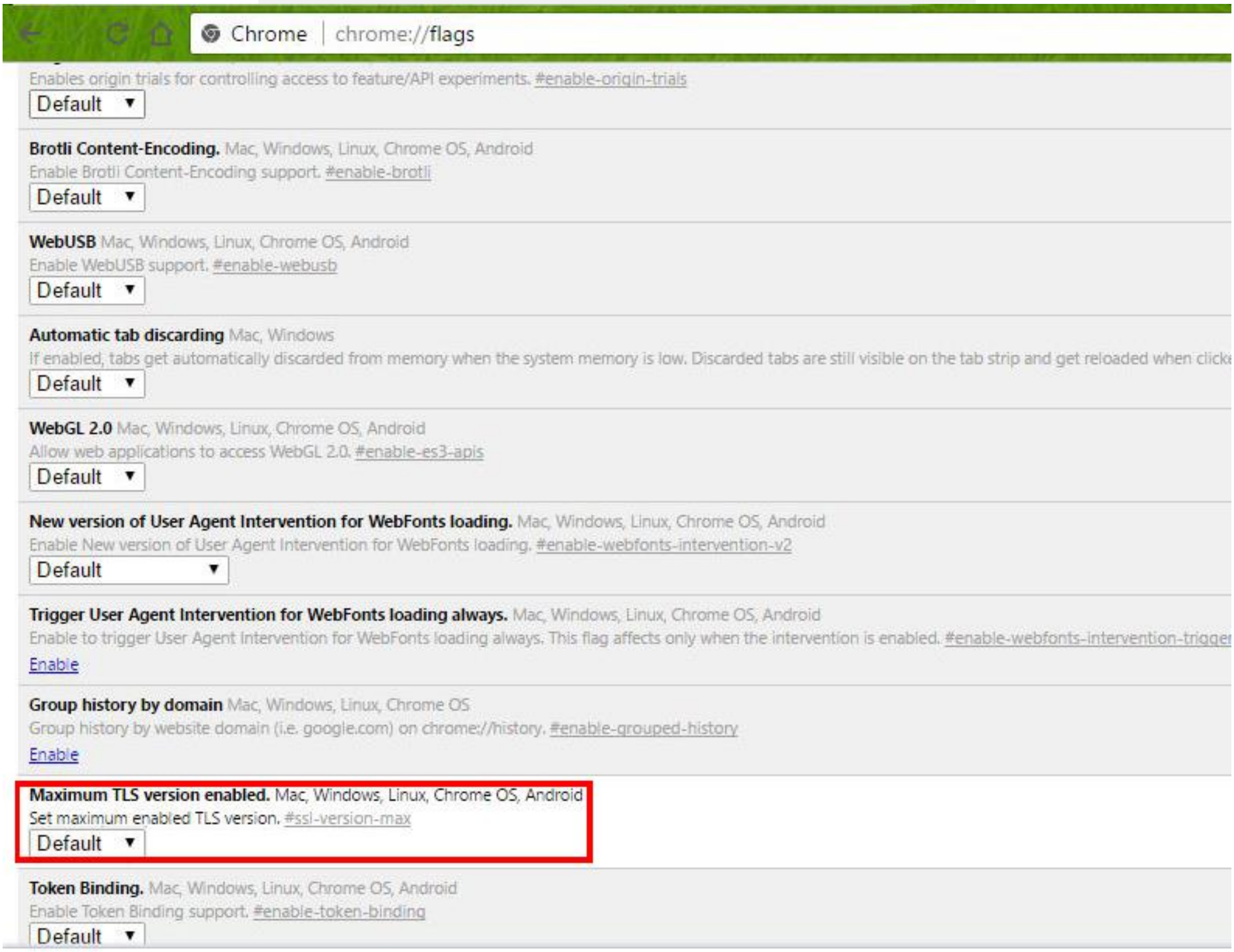
Careful, these experiments may bite

WARNING These experimental features may change, break or disappear at any time. We make absolutely no guarantees about what may happen if you turn one of these experiments on, and your browser may even spontaneously combust. Jokes aside, your browser may delete all your data or your security and privacy could be compromised in unexpected ways. Any experiments that you enable will be enabled for all users of this browser. Please proceed with caution. Interested in cool new Chrome features? Try our beta channel at chrome.com/beta.

Underneath this warning are all of the ‘experimental bits’, if you perform a search on the page for **TLS**.



TLS 1 of 2



Enables origin trials for controlling access to feature/API experiments. #enable-origin-trials
Default ▼

Brotli Content-Encoding. Mac, Windows, Linux, Chrome OS, Android
Enable Brotli Content-Encoding support. #enable-brotli
Default ▼

WebUSB Mac, Windows, Linux, Chrome OS, Android
Enable WebUSB support. #enable-webusb
Default ▼

Automatic tab discarding Mac, Windows
If enabled, tabs get automatically discarded from memory when the system memory is low. Discarded tabs are still visible on the tab strip and get reloaded when clicke
Default ▼

WebGL 2.0 Mac, Windows, Linux, Chrome OS, Android
Allow web applications to access WebGL 2.0. #enable-es3-apis
Default ▼

New version of User Agent Intervention for WebFonts loading. Mac, Windows, Linux, Chrome OS, Android
Enable New version of User Agent Intervention for WebFonts loading. #enable-webfonts-intervention-v2
Default ▼

Trigger User Agent Intervention for WebFonts loading always. Mac, Windows, Linux, Chrome OS, Android
Enable to trigger User Agent Intervention for WebFonts loading always. This flag affects only when the intervention is enabled. #enable-webfonts-intervention-trigge
Enable

Group history by domain Mac, Windows, Linux, Chrome OS
Group history by website domain (i.e. google.com) on chrome://history. #enable-grouped-history
Enable

Maximum TLS version enabled. Mac, Windows, Linux, Chrome OS, Android
Set maximum enabled TLS version. #ssl-version-max
Default ▼

Token Binding. Mac, Windows, Linux, Chrome OS, Android
Enable Token Binding support. #enable-token-binding
Default ▼

In the **Maximum TLS version enabled** change the value to **TLS 1.3** this will mean that as more services are able to make use of the latest security protocol, you computer will be already enabled to communicate this way.

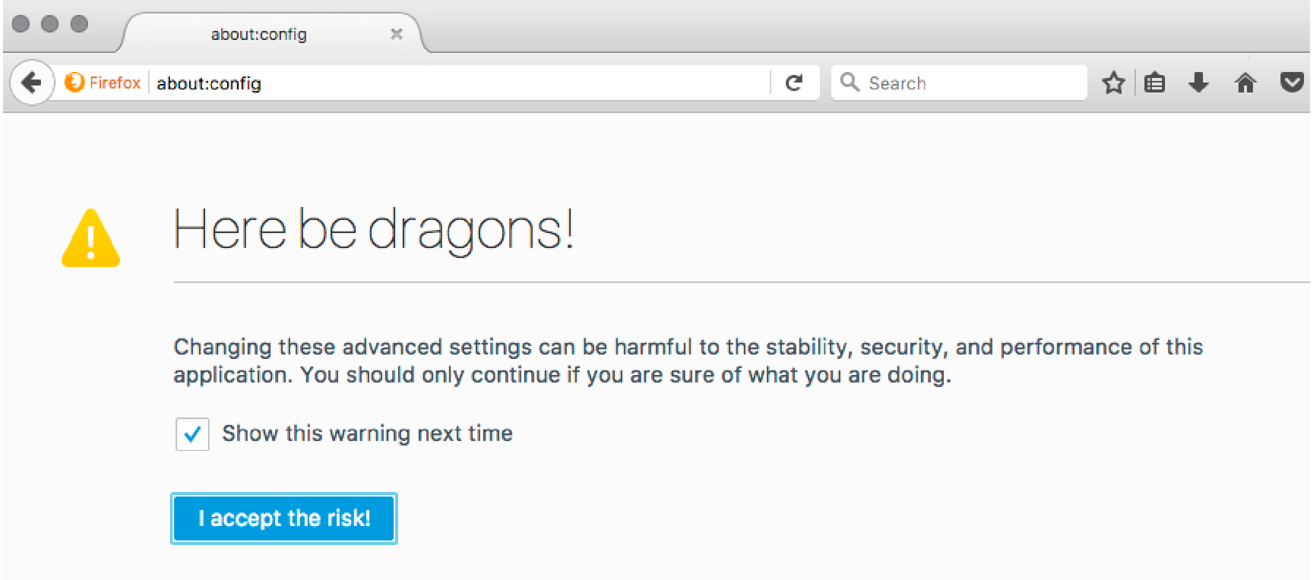
Google doesn't have a native equivalent of a minimum version of TLS that is supports in these settings.

If you are using a Windows computer, you can click on the three vertical dots in the top-right hand side of your Chrome window to access **Settings** (or you could type chrome://settings in your address bar) and scroll down to the bottom and select the hidden **Advanced Settings**.
If you scroll down to the **Network** section and click **Change proxy settings** you will be presented with the same information as presented in the **Internet Options** *section*.

Mozilla Firefox

On a computer, change your Internet browser settings through ***Firefox***.
Please note: these changes will only affect the use of Firefox itself, the changes will not be reflected for all other Internet browsers on your computer.

To access the Firefox settings, in the address bar type: **about:config** and you will be presented with a warning screen depicted below.

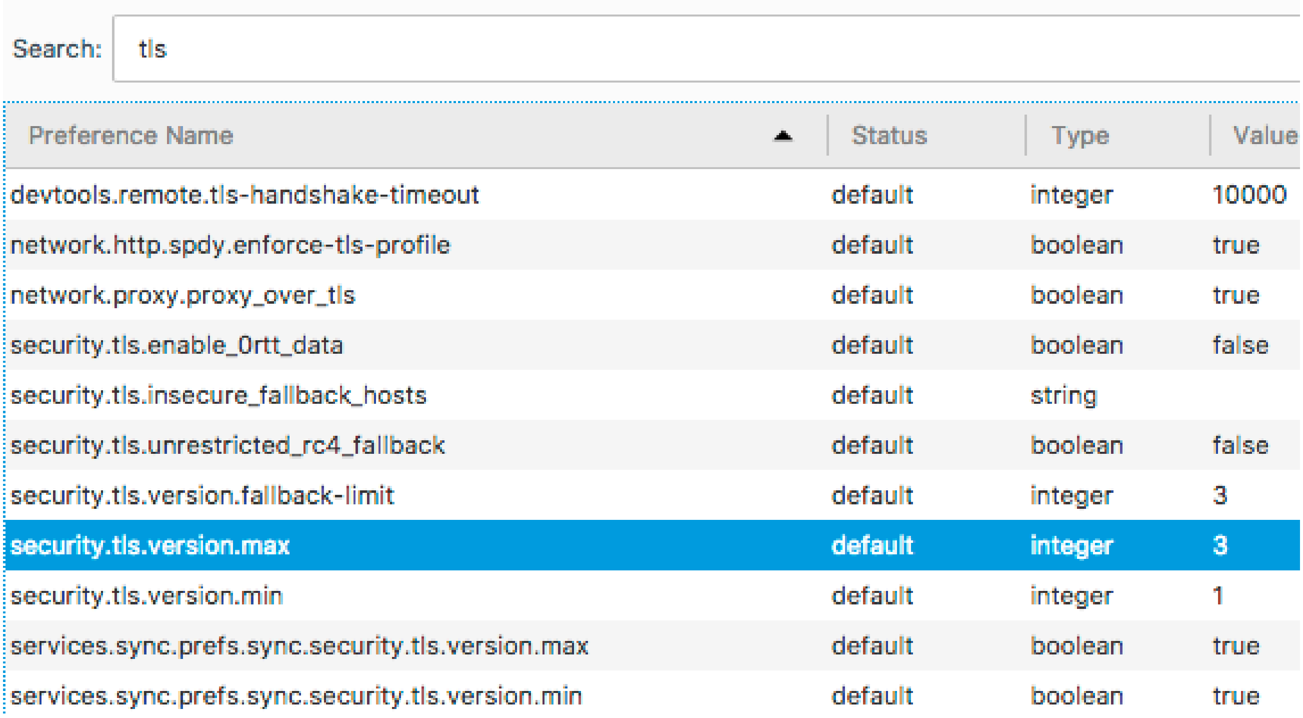


Here be dragons!

Changing these advanced settings can be harmful to the stability, security, and performance of this application. You should only continue if you are sure of what you are doing.

☑ Show this warning next time

Click the accept the risk button and you will be presented with a long list of settings. In the search bar type **TLS**, you will then be presented the options to change.



Search: tls

Preference Name	Status	Type	Value
devtools.remote.tls-handshake-timeout	default	integer	10000
network.http.spdy.enforce-tls-profile	default	boolean	true
network.proxy.proxy_over_tls	default	boolean	true
security.tls.enable_0rtt_data	default	boolean	false
security.tls.insecure_fallback_hosts	default	string	
security.tls.unrestricted_rc4_fallback	default	boolean	false
security.tls.version.fallback-limit	default	integer	3
security.tls.version.max	default	integer	3
security.tls.version.min	default	integer	1
services.sync.prefs.sync.security.tls.version.max	default	boolean	true
services.sync.prefs.sync.security.tls.version.min	default	boolean	true

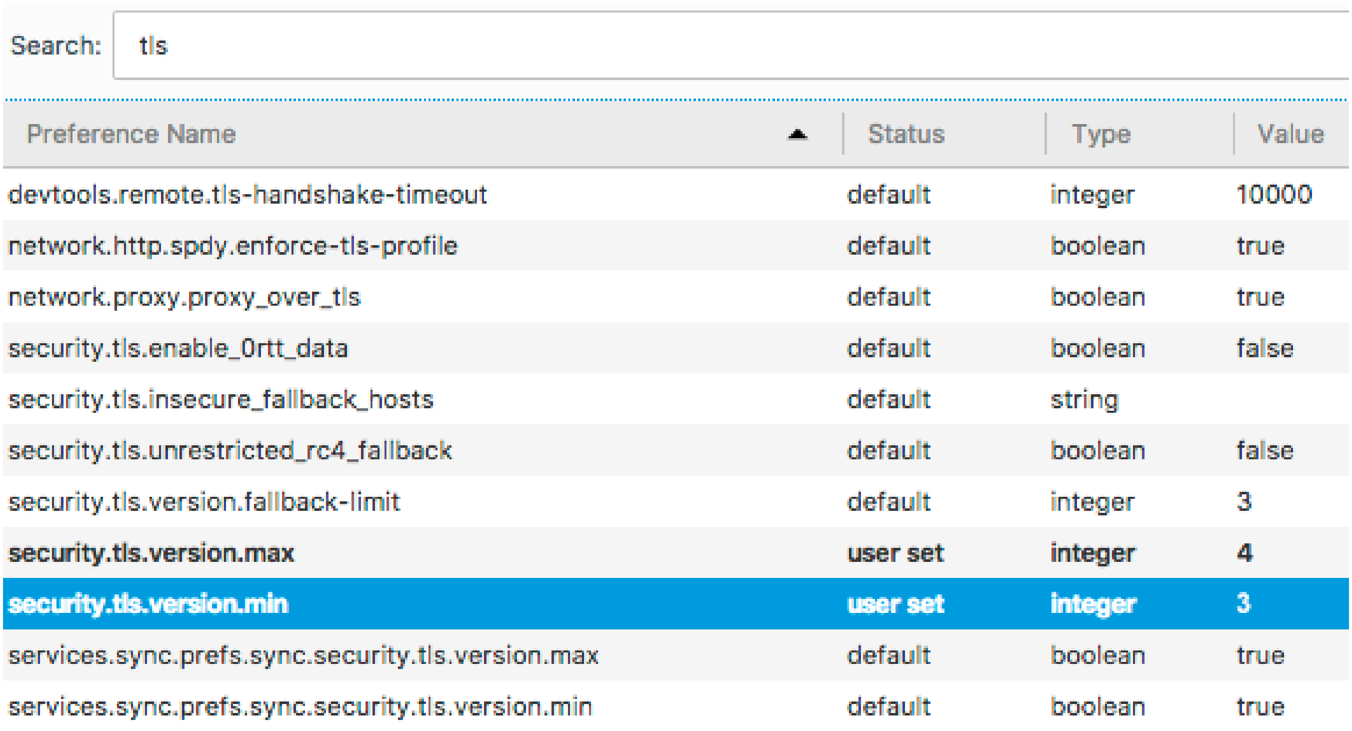
The values are as follows:

1	TLS 1.0
2	TLS 1.1
3	TLS 1.2
4	TLS 1.3

Double click the **security.tls.version.max** and in the dialogue box type **4** – this will provide the greatest longevity for your browser. If you have recently installed Firefox, this value will already be set.

Double click the **security.tls.version.min** and in the dialogue box type **3** – this will provide the greatest safe option for your browser at this point in time. You may need to drop this value down to **2** if you encounter problems accessing some sites – but TLS 1.1 is not a long term option that is sustainable, as it will be removed from University services by the turn of the year.

You should now see the status settings have changed from default to user defined.

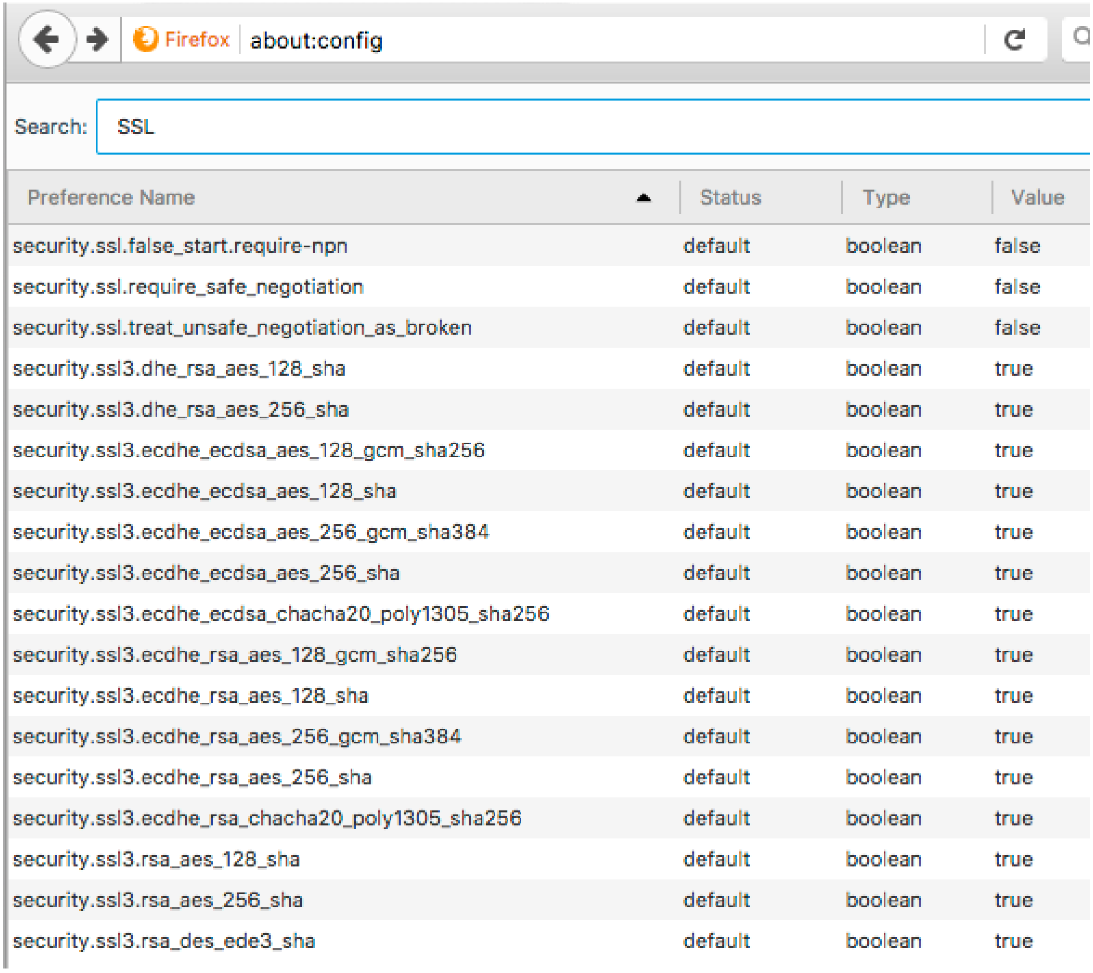


Search: tls

Preference Name	Status	Type	Value
devtools.remote.tls-handshake-timeout	default	integer	10000
network.http.spdy.enforce-tls-profile	default	boolean	true
network.proxy.proxy_over_tls	default	boolean	true
security.tls.enable_0rtt_data	default	boolean	false
security.tls.insecure_fallback_hosts	default	string	
security.tls.unrestricted_rc4_fallback	default	boolean	false
security.tls.version.fallback-limit	default	integer	3
security.tls.version.max	**user set**	**integer**	**4**
security.tls.version.min	**user set**	**integer**	**3**
services.sync.prefs.sync.security.tls.version.max	default	boolean	true
services.sync.prefs.sync.security.tls.version.min	default	boolean	true

These settings will now be applied after closing Firefox and restarting the application.

Firefox also has the capability to manage the Cipher Suites that are available for use, if you change your search term to be **SSL** you will be presented with a long list of settings.



Search: SSL

Preference Name	Status	Type	Value
security.ssl.false_start.require-npn	default	boolean	false
security.ssl.require_safe_negotiation	default	boolean	false
security.ssl.treat_unsafe_negotiation_as_broken	default	boolean	false
security.ssl3.dhe_rsa_aes_128_sha	default	boolean	true
security.ssl3.dhe_rsa_aes_256_sha	default	boolean	true
security.ssl3.ecdhe_ecdsa_aes_128_gcm_sha256	default	boolean	true
security.ssl3.ecdhe_ecdsa_aes_128_sha	default	boolean	true
security.ssl3.ecdhe_ecdsa_aes_256_gcm_sha384	default	boolean	true
security.ssl3.ecdhe_ecdsa_aes_256_sha	default	boolean	true
security.ssl3.ecdhe_ecdsa_chacha20_poly1305_sha256	default	boolean	true
security.ssl3.ecdhe_rsa_aes_128_gcm_sha256	default	boolean	true
security.ssl3.ecdhe_rsa_aes_128_sha	default	boolean	true
security.ssl3.ecdhe_rsa_aes_256_gcm_sha384	default	boolean	true
security.ssl3.ecdhe_rsa_aes_256_sha	default	boolean	true
security.ssl3.ecdhe_rsa_chacha20_poly1305_sha256	default	boolean	true
security.ssl3.rsa_aes_128_sha	default	boolean	true
security.ssl3.rsa_aes_256_sha	default	boolean	true
security.ssl3.rsa_des_ede3_sha	default	boolean	true

Double click the **security.ssl3.rsa_des_ede3_sha** to change its value to false. This change should be made as the cipher suite is weak in terms of its security.

These settings will come into effect when your restart Firefox.