

TRANSPORT LAYER SECURITY (TLS) 1.2 REQUIRED BROWSER SETTINGS v1.0

OPEN ACCESS TECHNOLOGY INTERNATIONAL, INC.

MARCH 2020

PROPRIETARY AND CONFIDENTIAL

OPEN ACCESS TECHNOLOGY INTERNATIONAL, INC. 3660 Technology Drive NE | Minneapolis, MN 55418 | Phone 763.201.2000 | Fax 763.201.5333 | www.oati.com ©2020 Open Access Technology International, Inc.

TRADE SECRET

This document and attachments contain confidential and proprietary information of Open Access Technology International, Inc. This information is not to be used, disseminated, distributed, or otherwise transferred without the expressed written permission of Open Access Technology International, Inc.

PROPRIETARY NOTICE

OATI webSupport is a trademark and service mark of Open Access Technology International, Inc. All rights reserved.

Table of Contents

1.	Introduction	. 4
2.	Internet Explorer (IE)	. 5
	2.1 How to View or Change the TLS Settings in IE2.2 How to Find the TLS Version Used in IE	. 5 . 6
3.	Microsoft Edge	. 7
	3.1 How to View or Change the TLS Settings in Microsoft Edge3.2 How to Find the TLS Version Used in Microsoft Edge	.7 .8
4.	Google Chrome (Lower than Release 81)	. 9
	4.1 How to View or Change the TLS Settings in Google Chrome4.2 How to Find the TLS Version Used in Google Chrome	. 9 10
5.	Mozilla Firefox	11
	5.1 How to View or Change the TLS Settings in Mozilla Firefox5.2 How to find the TLS version used in Mozilla Firefox	11 11

1. Introduction

This document describes the Transport Layer Security (TLS) settings for common internet browsers. Included for each browser is how to view and change the TLS settings to support TLS version 1.2 and how to check the TLS version when accessing a web site. Note: these browser settings may be controlled by Group Policy and users may not be able to change them.

2. Internet Explorer (IE)

2.1 How to View or Change the TLS Settings in IE

- 1. Open IE.
- 2. From the menu bar, click Tools > Internet Options > Advanced tab.
- 3. Scroll down to Security category, manually check the option box for Use TLS 1.2.

😪 Internet Properties ? X								
General Security	Privacy	Content	Connections	Programs	Advar	nced		
Settings						_		
Enable DOM Storage Enable Enhanced Protected Mode* Enable Integrated Windows Authentication* Enable Integrated Windows Authentication* Enable native XMLHTTP support Enable Windows Defender SmartScreen Send Do Not Track requests to sites you visit in Internet E Use SSL 3.0 Use SSL 3.0 Use TLS 1.1 Use TLS 1.1 Use TLS 1.1 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 n								
< *Takes effect	after you	restart vo	ir computer		>			
Takes effect	arter you	restart you	Restore	advanced s	settings			
Reset Internet Explorer settings								
Resets Internet Explorer's settings to their default Reset								
You should only use this if your browser is in an unusable state.								
		Oł	(Ca	ancel	Арр	ly		

- 4. Click on the "OK" button.
- 5. Close your browser and restart Internet Explorer.

2.2 How to Find the TLS Version Used in IE

- 1. Launch the Internet Explorer.
- 2. Enter the Uniform Resource Locater (URL) you wish to check in the browser.
- 3. Right-click the page or select the Page drop-down menu, and select Properties.
- 4. In the new window, look for the Connection section. This will describe the version of TLS or Secured Socket Layer (SSL) used.

Properties	>					
General						
2	OATI webSupport 5.0					
Protocol:	HyperText Transfer Protocol with Privacy					
Type:	HTML Document					
Connection: TLS 1.2, AES with 256 bit encryption (High); ECDH with 255 bit exchange						
Zone:	Trusted sites Protected Mode: Off					
Address: (URL)	https://websupport.oati.com/websupport/SupportMai n.wml					
Size:	Not Available					
Created:	Not Available					
Modified:	Not Available					
	Certificates					
	OK Cancel Apply					
	©2020 OATI. I					

3. Microsoft Edge

3.1 How to View or Change the TLS Settings in Microsoft Edge

- 1. In the Windows menu search box, type Internet options.
- 2. Under Best match, click Internet Options.
- 3. In the Internet Properties window, on the Advanced tab, scroll down to the Security section.

♠ Internet Properties ? ×									
General Security	Privacy Conter	t Connections	Programs	Advan	ced				
Settings									
Settings Enable DOM Storage Enable Enhanced Protected Mode* Enable Integrated Windows Authentication* Enable Integrated Windows Authentication* Enable Windows Defender SmartScreen Send Do Not Track requests to sites you visit in Internet E Use SSL 3.0 Use TLS 1.0 Use TLS 1.1 Varn about certificate address mismatch* Warn about certificate address mismatch* Warn if changing between secure and not secure mode Warn if CoST submittal is redirected to a zone that does a									
<	-			>					
*Takes effect	after you restart	our computer							
		Restore	e advanced s	ettings					
Reset Internet Explorer settings									
Resets Internet Explorer's settings to their default Reset									
You should only use this if your browser is in an unusable state.									
		ок с	ancel	App	ly				

- 4. Check the User TLS 1.2 checkbox.
- 5. Click on the "OK" button.
- 6. Close your browser and restart Microsoft Edge browser.

3.2 How to Find the TLS Version Used in Microsoft Edge

- 1. Press CTRL+SHIFT+i.
- 2. Click on the "Security Tab".
- 3. View under "Connection" section.

Security overview
This page is secure (valid HTTPS).
Certificate - valid and trusted
The connection to this site is using a valid, trusted server certificate issued by webCARES Issuing CA 2017.
View certificate
 Connection - secure connection settings
The connection to this site is encrypted and authenticated using TLS 1.2, ECDHE_RSA with X25519, and AES_256_GCM.
Resources - all served securely
All resources on this page are served securely.
©2020 OATI, Inc.

4. Google Chrome (Lower than Release 81)

4.1 How to View or Change the TLS Settings in Google Chrome

- 1. In the Windows menu search box, type Internet options.
- 2. Under Best match, click Internet Options.
- 3. In the Internet Properties window, on the Advanced tab, scroll down to the Security section.

🐏 Internet Properties ?							×		
General	Security	Privacy	Content	Connections	Programs	Advan	ced		
Settings									
Settings Enable DOM Storage Enable Enhanced Protected Mode* Enable Integrated Windows Authentication* Enable Integrated Windows Authentication* Enable Windows Defender SmartScreen Send Do Not Track requests to sites you visit in Internet E Use SSL 3.0 Use TLS 1.0 Use TLS 1.1 Vise TLS 1.2 Vise TLS									
<						>			
*Ta	kes effect a	after you	restart you	ir computer					
				Restore	advanced s	ettings			
Reset Internet Explorer settings									
Resets Internet Explorer's settings to their default Reset									
You should only use this if your browser is in an unusable state.									
			Ok	Ca	ancel	Appl	у		

- 4. Check the User TLS 1.2 checkbox.
- 5. Click on the "OK" button.
- 6. Close your browser and restart Google Chrome.

NOTE: Starting with the release of Chrome 81, users won't be able to connect with sites that have not upgraded to TLS 1.2.

4.2 How to Find the TLS Version Used in Google Chrome

- 1. Press CTRL+SHIFT+i.
- 2. Click on the "Security Tab"/
- 3. View under "Connection" section.

Security overview
This page is secure (valid HTTPS).
Certificate - valid and trusted
The connection to this site is using a valid, trusted server certificate issued by webCARES Issuing CA 2017.
View certificate
 Connection - secure connection settings
The connection to this site is encrypted and authenticated using TLS 1.2, ECDHE_RSA with X25519, and AES_256_GCM.
Resources - all served securely
All resources on this page are served securely.
©2020 OATI, Inc.

5. Mozilla Firefox

5.1 How to View or Change the TLS Settings in Mozilla Firefox

- 1. Open Firefox
- 2. In the address bar, type "about:config" and press "Enter" button.
- 3. In the Search field, enter "tls". Find and double-click the entry for "security.tls.version.min".
- 4. Set the integer value to 3 to force protocol of TLS 1.2 to be the default.

Advanced Preferences X +			- a x
← → C ⊕ Ø Firefox aboutconfg		Ŷ	⊮\© 37 ≣
o tis			
devtools.remote.tis-handshake-timeout	10000		1
gluse-tis-is-current	0		
media.peerconnection.dt/s.version.max	771		1
media.peerconnection.dt/s.version.min	770		1
network:http.spdy.enforce-tis-profile	true		⇒
network.http.tls-handshake-timeout	30		
network.proxy.proxy_over_tls	true		⇒
security.tls.enable_0rtt_data	true		72
security/l/senable_delegated_credentials	false		*
security.tls.enable_post_handshake_auth	false		≠
security.tls.hello_downgrade_check	true		-
security.tls.insecure_fallback_hosts			1
security.tls.version.enable-deprecated	false		=
security.tls.version.fallback-limit	4		-
security.tlis.version.max	4		
security.tfs.version.min	1 Q		1 .
tha	Boolean ONumber OString		+

- 5. Click on the "OK" button.
- 6. Close your browser and restart Mozilla Firefox.

5.2 How to find the TLS version used in Mozilla Firefox

- 1. Launch Firefox.
- 2. Enter the URL you wish to check in the browser.
- 3. In the address bar, click the icon to the left of the URL.
- 4. Click on the arrow to the right.



This document contains proprietary and confidential information of OATI, Inc. Do not copy or distribute without explicit permission of OATI, Inc. ©2020 Open Access Technology International, Inc.

©2020 OATI, Inc.

5. View Technical Details

ۏ Page Info	- https://	websupport.oa	ti.com/websupport/	views/login.wml?tim	edo	_		\times
<u>G</u> eneral	LE Media	† ŏ <u>P</u> ermissions	Security					
Website Ide	entity							
Website:	websup	port.oati.com						
Owner:	This we	bsite does not s	supply ownership inf	ormation.				
Verified by:	Open A	ccess Technolo	gy International Inc			Viev	v Certific	ate
Expires on:	Saturda	y, December 19	, 2020					
Privacy & Hi	istory							
Have I visited	d this web	osite prior to to	day?	No				
Is this websit	te storing	information or	n my computer?	No	<u>C</u> lear C	ookies a	nd Site D	ata
Have I saved	any pass	words for this v	vebsite?	No	Vi	/ie <u>w</u> Saved Passwords		
Technical De Connection The page yo Encryption n therefore un	e tails Encrypted u allosviev nakes it d likely that	d (TLS_ECDHE_ ving was encry ifficult for unau t anyone read t	RSA_WITH_AES_256_ oted before being tra uthorized people to v his page as it traveled	GCM_SHA384, 256 bi nsmitted over the In iew information trav d across the network.	it keys, Ti ternet. eling bet	LS 1.2) ween co	mputers. Help	It is
							e2020.0	

Filename: OATI TLS 1.2 Required Browser Settings v1.0 CS 031120