Upcoming Change - Deactivation of Transport Layer Security (TLS) 1.0

Summary

Washington State Department of Health (DOH), in cooperation with our Internet Service Provider, Washington Technology Solutions (WaTech), will be deactivating Transport Layer Security (TLS) 1.0. This change will take place in our production Fortress Anonymous Gateway environment on January 1, 2019. Fortress Anonymous is the environment that hosts the application that you are accessing.

What do I need to do?

Most modern browsers are already set to handle the newer TLS protocol settings. To avoid potential disruption when accessing web applications end users must be using compliant browsers before January 1, 2019.

To enable TLS 1.1 and/or TLS 1.2 protocols on web browsers, see the instructions below.

- Microsoft Internet Explorer
- Microsoft Edge
- Google Chrome
- Mozilla Firefox
- Opera
- Apple Safari

Anyone connecting to DOH services using 3rd-party applications that do not support TLS 1.1 or higher must upgrade those applications to support TLS 1.1 or higher before January 1, 2019. This must be done in order to avoid issues.

What is TLS?

Transport Layer Security is a widely used security protocol to securely exchange data over a network. TLS ensures a connection to a remote endpoint through encrypted identity verification. The available versions are TLS 1.0, 1.1 and 1.2. The environment that hosts this application uses TLS as a key component of its security.

Why is TLS 1.0 being disabled?

WaTech is upgrading the Fortress Anonymous Gateway to TLS 1.1 and higher in order to align with industry best practices. WaTech and DOH are focused on continually helping our customers improve security by using the latest security protocols.

What happens after TLS 1.0 is disabled?

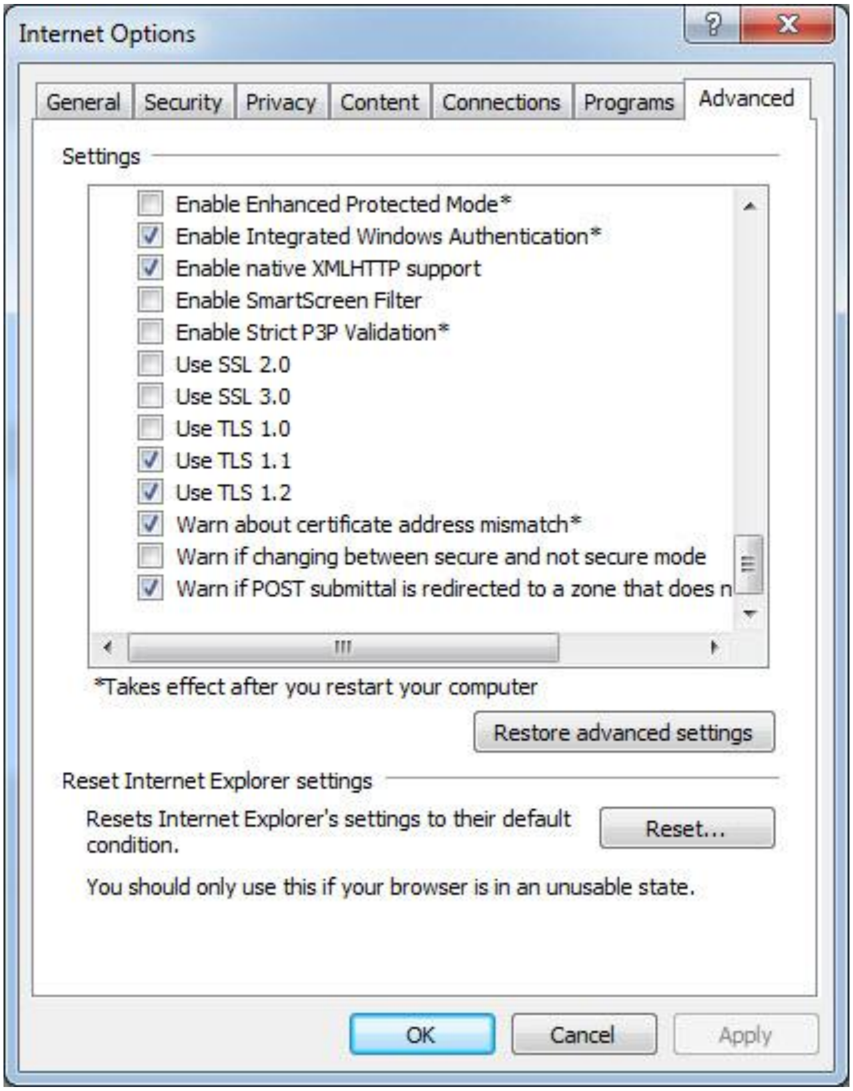
Browsers that rely solely on the TLS 1.0 protocol will have issues accessing DOH applications.

Third party applications that connect to DOH services that use the TLS 1.0 protocol will experience issues.

Enabling TLS 1.1 and TLS 1.2 on web browsers

Microsoft Internet Explorer

1. Open Internet Explorer
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 1.1 and Use TLS 1.2



Settings

☐ Enable Enhanced Protected Mode*
☑ Enable Integrated Windows Authentication*
☑ Enable native XMLHTTP support
☐ Enable SmartScreen Filter
☐ Enable Strict P3P Validation*
☐ Use SSL 2.0
☐ 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 n

*Takes effect after you restart your computer

Reset Internet Explorer settings

Resets Internet Explorer's settings to their default condition.

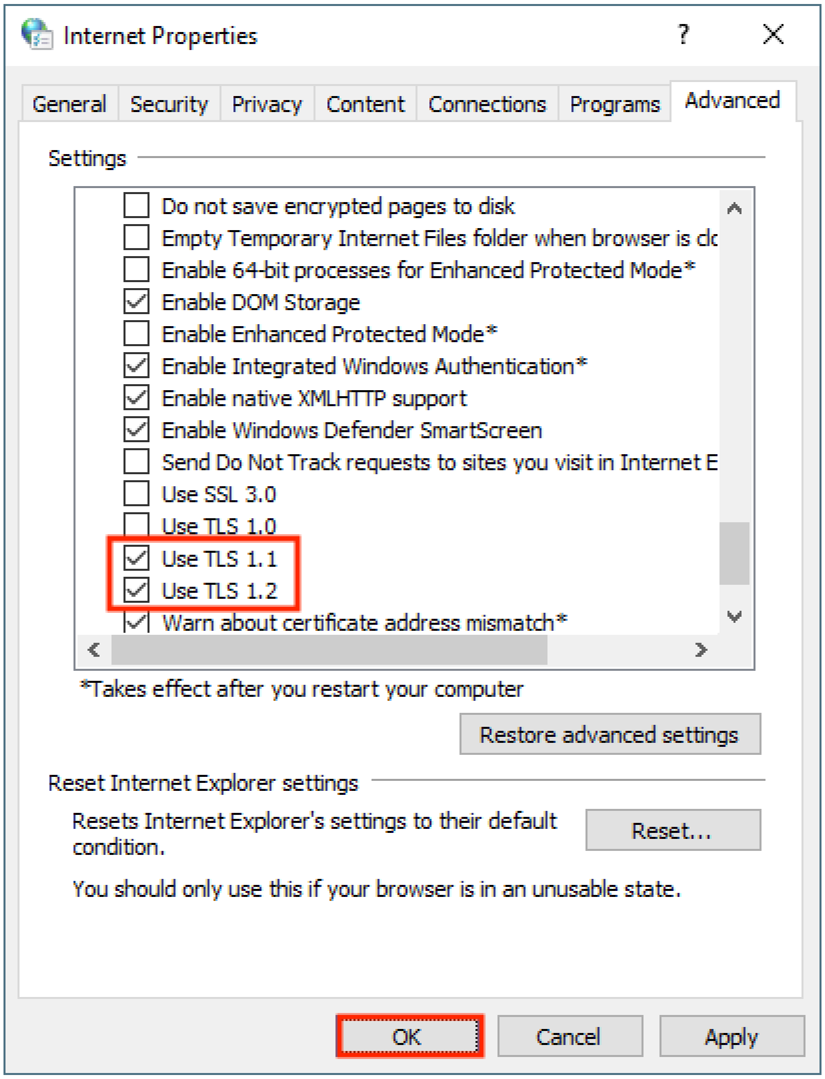
You should only use this if your browser is in an unusable state.

4. Click OK.
5. Close your browser and restart Internet Explorer.

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 Advance tab, scroll down to the Security section.



- ☐ Do not save encrypted pages to disk
- ☐ Empty Temporary Internet Files folder when browser is clc
- ☐ Enable 64-bit processes for Enhanced Protected Mode*
- ☑ Enable DOM Storage
- ☐ Enable Enhanced Protected Mode*
- ☑ 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 TLS 1.0
- ☑ Use TLS 1.1
- ☑ Use TLS 1.2
- ☑ Warn about certificate address mismatch*

*Takes effect after you restart your computer

Reset Internet Explorer settings

Resets Internet Explorer's settings to their default condition.

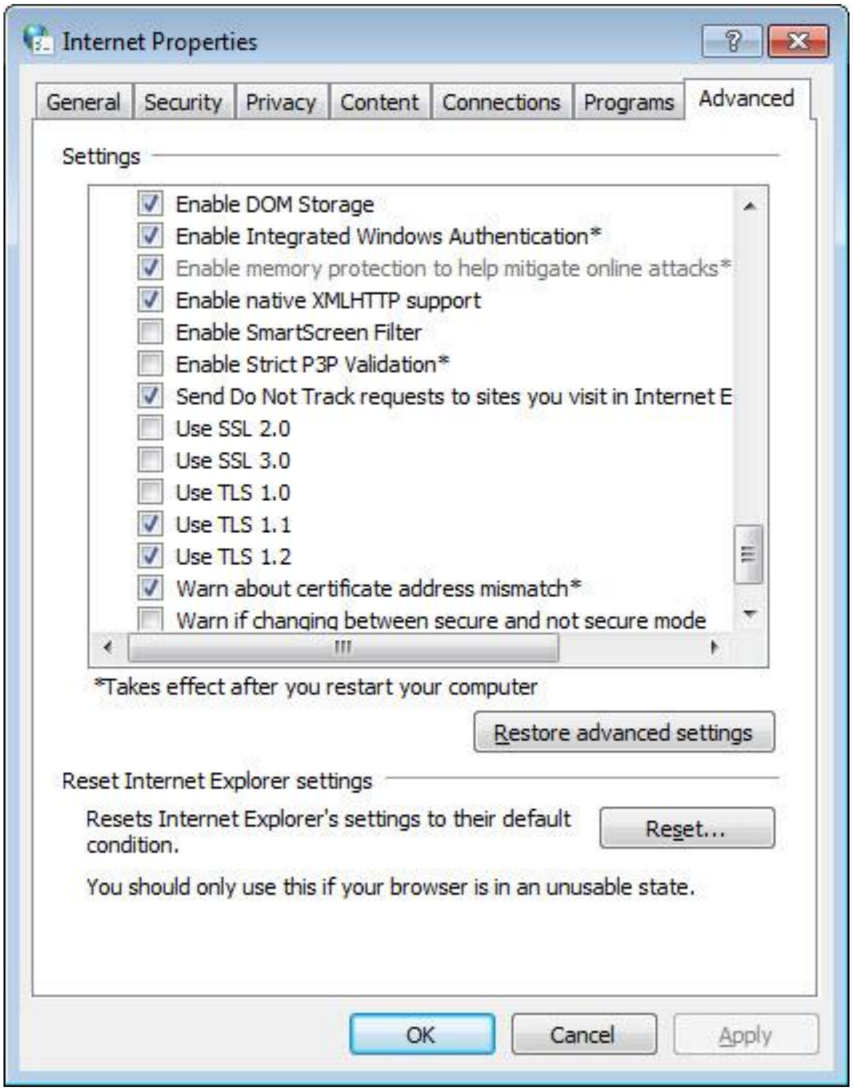
You should only use this if your browser is in an unusable state.

4. Check the Use TLS 1.1 and User TLS 1.2 check boxes.
5. Click OK.
6. Close your browser and restart Microsoft Edge browser.

Google Chrome

1. Open Google Chrome
2. Click Alt F and select Settings
3. Scroll down and expand the Advanced settings menu.
4. Scroll down to the System section and click on Open proxy settings.
5. Select the Advanced tab

6. Scroll down to Security category, manually check the option box for Use TLS 1.1 and Use TLS 1.2



Settings

☑ Enable DOM Storage
☑ Enable Integrated Windows Authentication*
☑ Enable memory protection to help mitigate online attacks*
☑ Enable native XMLHTTP support
☐ Enable SmartScreen Filter
☐ Enable Strict P3P Validation*
☑ Send Do Not Track requests to sites you visit in Internet E
☐ Use SSL 2.0
☐ 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

*Takes effect after you restart your computer

Reset Internet Explorer settings

Resets Internet Explorer's settings to their default condition.

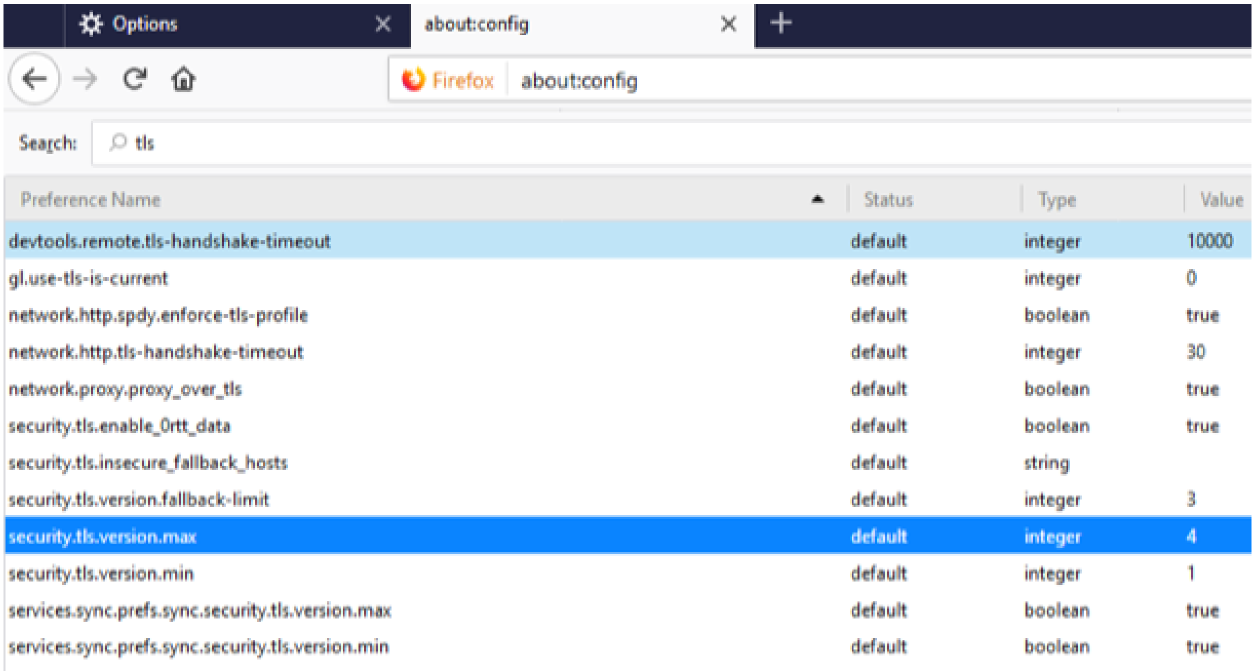
You should only use this if your browser is in an unusable state.

7. Click OK
8. Close your browser and restart Google Chrome

Mozilla Firefox

1. Open Firefox
2. In the address bar, type about:config and press Enter
3. In the Search field, enter tls. Find and double-click the entry for security.tls.version.max

4. Set the integer value to 4 to force a maximum protocol of TLS 1.3.



Search: tls

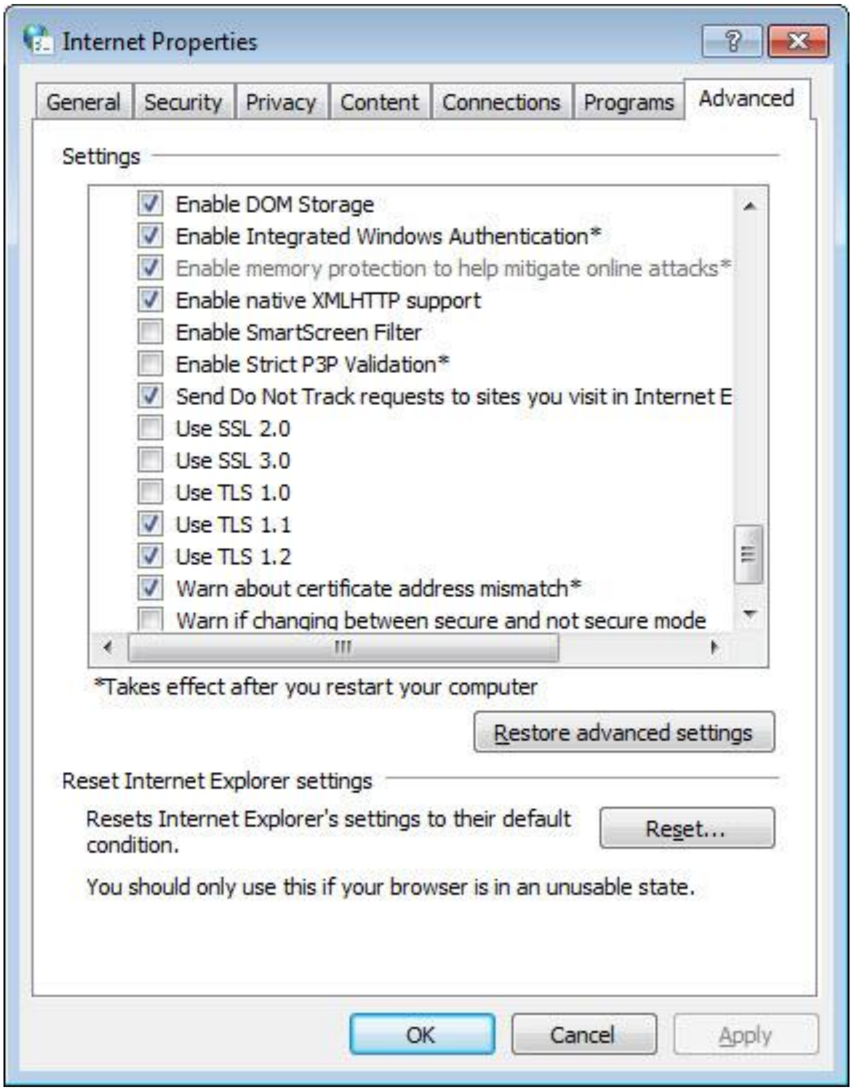
Preference Name	Status	Type	Value
devtools.remote.tls-handshake-timeout	default	integer	10000
gl.use-tls-is-current	default	integer	0
network.http.spdy.enforce-tls-profile	default	boolean	true
network.http.tls-handshake-timeout	default	integer	30
network.proxy.proxy_over_tls	default	boolean	true
security.tls.enable_0rtt_data	default	boolean	true
security.tls.insecure_fallback_hosts	default	string	
security.tls.version.fallback-limit	default	integer	3
security.tls.version.max	default	integer	4
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

5. Click OK
6. Close your browser and restart Mozilla Firefox

Opera

1. Open Opera
2. Click Ctrl plus F12
3. Scroll down to the Network section and click on Change proxy settings.
4. Select the Advanced tab

5. Scroll down to Security category, manually check the option box for Use TLS 1.1 and Use TLS 1.2



Settings

- ☑ Enable DOM Storage
- ☑ Enable Integrated Windows Authentication*
- ☑ Enable memory protection to help mitigate online attacks*
- ☑ Enable native XMLHTTP support
- □ Enable SmartScreen Filter
- □ Enable Strict P3P Validation*
- ☑ Send Do Not Track requests to sites you visit in Internet E
- □ Use SSL 2.0
- □ 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

*Takes effect after you restart your computer

Reset Internet Explorer settings

Resets Internet Explorer's settings to their default condition.

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

6. Click OK
7. Close your browser and restart Opera

Apple Safari

There are no options for enabling SSL protocols. If you are using Safari version 7 or greater, TLS 1.1 and TLS 1.2 are automatically enabled.