FireLight Security Changes

To align with industry best practices for security and data integrity, Insurance Technologies will be implementing the following security changes for the 2.11 release slated for October 2017. This article contains all of the information currently available on the reasoning and timing of the change.

TLS 1.0 Support

To align with industry best practices for security and data integrity, Insurance Technologies is requiring an upgrade to TLS 1.1 or higher by October 27, 2017.

What is TLS?

TLS is acronym for "Transport Layer Security". TLS is a protocol used to establish a secure connection between two servers with the intent to provide data integrity and privacy. The protocol is used both inbound between a client's browser and the FireLight hosting environment servers, and outbound between FireLight hosting servers and our client's back office endpoints. TLS ensures that a connection to the remote endpoint is the intended endpoint through encryption and endpoint identity verification. To date, the current versions of TLS include TLS 1.0, 1.1, and 1.2.

What is the change?

Insurance Technologies will gradually deprecate support for TLS 1.0 within all FireLight hosting environments by October 31, 2017. We will continue to support TLS 1.1 and TLS 1.2. This will be a phased implementation starting with QE, then UAT, and finally Staging and Production. Listed below is the planned schedule:

- September 5, 2017 - Security test page (https://tlstest.insurancetechnologies.com)
- September 5, 2017 - External QE (e.g. https://firelight.insurancetechnologies.com)
- September 29, 2017 - UAT (e.g. https://uat.firelighteapp.com)
- October 27, 2017 - Staging (e.g. https://staging.firelighteapp.com)
- October 27, 2017 - Production (e.g. https://www.firelighteapp.com)

What is the impact?

After the change, any users connecting to any of the above environments using TLS 1.0 will receive a notification page indicating stronger security is required to access the site. The page will provide information on how to adjust their security settings, or how to upgrade to a browser supported by FireLight.

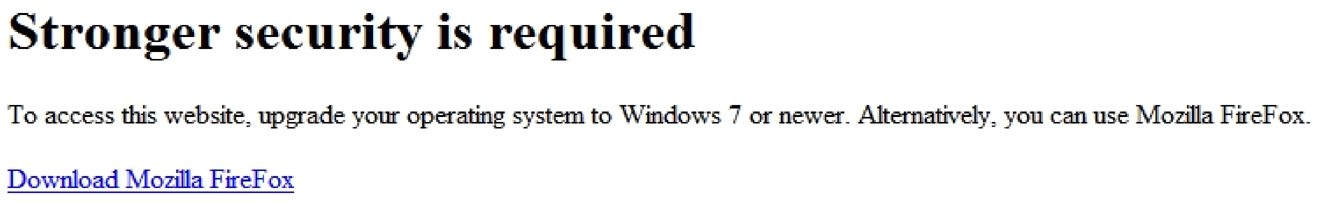
For outbound connectivity, the transmission of application data and attachments will fail until the endpoint accepts TLS 1.1 or TLS 1.2. If your back office servers cannot support the higher protocols by the dates noted above, please contact your product manager for alternative solutions.

Agent and Client impact?

The agent or user using a browser to access FireLight using the TLS 1.0 protocol will see one of several responses depending on the operating system and browser used. Listed below are the possible responses:

Windows XP and IE

The following page will be displayed:



Stronger security is required

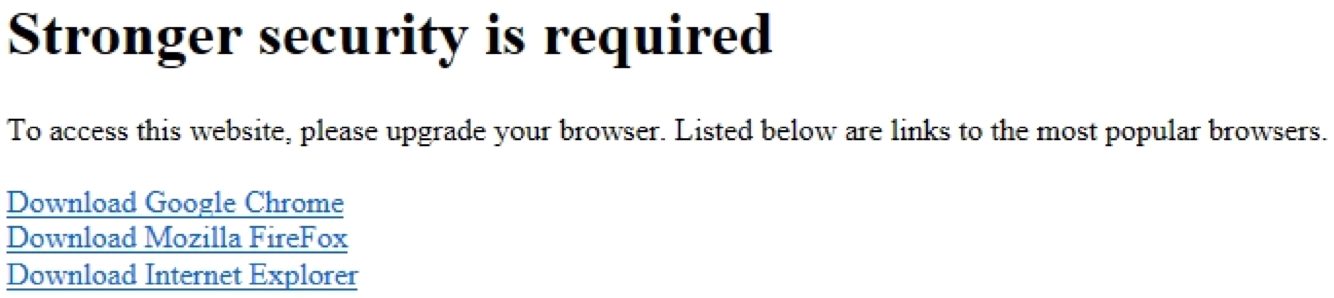
To access this website, upgrade your operating system to Windows 7 or newer. Alternatively, you can use Mozilla FireFox.

Download Mozilla FireFox

A link will be provide to download FireFox.

Other O/S and Browser

The following page will be displayed:



Stronger security is required

To access this website, please upgrade your browser. Listed below are links to the most popular browsers.

Download Google Chrome
Download Mozilla FireFox
Download Internet Explorer

The page will provide links to the latest version of each major browser.

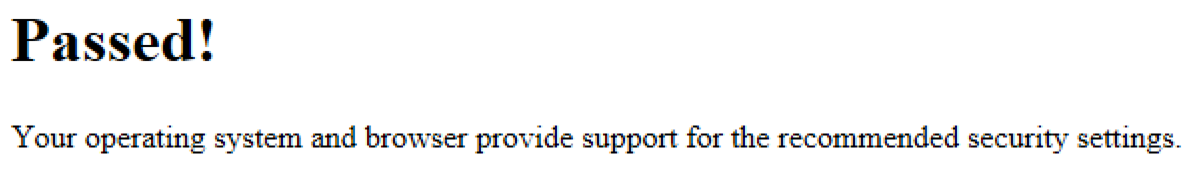
Browser Compatibility

The table below lists the major browsers and their support for TLS 1.1 and TLS 1.2 protocols:

Browser	Compatibility Notes
Microsoft Internet Explorer (IE)	
Desktop and mobile IE, version 11	Compatible with TLS 1.1 and above by default.

	If you see the message “Stronger security is required”, you may need to turn off TLS 1.0 setting in the Internet Options|Advanced Setting dialog.
Desktop IE, versions 8,9, and 10	Compatible when running Windows 7 or above operating system, but not enabled by default. Review the Enabling TLS 1.1 and TLS 1.2 article for directions to enable the higher protocols.
Desktop IE, versions 7 and below	Not compatible with TLS 1.1 or higher.
Mobile IE, versions 10 and below	Not compatible with TLS 1.1 or higher.
Microsoft Edge	Compatible with TLS 1.1 and higher
Mozilla FireFox	Most versions compatible with TLS 1.1 and higher, regardless of operating system.
FireFox, 27 and higher	Compatible with TLS 1.1 or higher. Enabled by default.
FireFox, version 23 through 26	Compatible with TLS 1.1 or higher, but not enabled by default.
Google Chrome	Most versions compatible with TLS 1.1 or higher, regardless of operating system.
Chrome, version 38 and higher	Compatible with TLS 1.1 or higher. Enabled by default.
Chrome, version 22 through 27	Compatible when running Windows XP, SP3, Vista, or newer Microsoft desktop operating system. Compatible when running Mac OS X 10.6 or newer desktop operating system.
Chrome, version 21 and below	Not compatible with TLS 1.1 or higher.
Apple Safari	
Safari, version 7 and higher	Compatible with TLS 1.1 or higher when running on OS X 10.9 and higher. Enabled by default.
Safari, version 6 and below	Not compatible with TLS 1.1 or higher.
Mobile Safari, version 5 and higher	Compatible with TLS 1.1 or higher when running on iOS 5 and higher. Enabled by default.
Mobile Safari, version 4 and below	Not compatible with TLS 1.1 or higher.

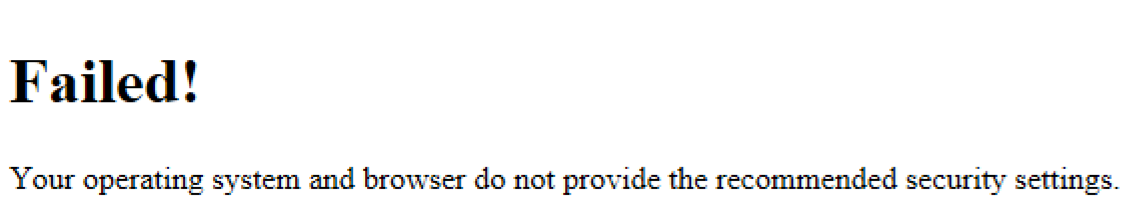
If you are unsure of the browser and operating system information, browse to https://tlstest.insurancetechnologies.com to test compatibility. If you receive the following response, your configuration is compatible with the new security requirements.



Passed!

Your operating system and browser provide support for the recommended security settings.

If you receive the following response, your configuration is not compatible with the new security requirements.



Failed!

Your operating system and browser do not provide the recommended security settings.

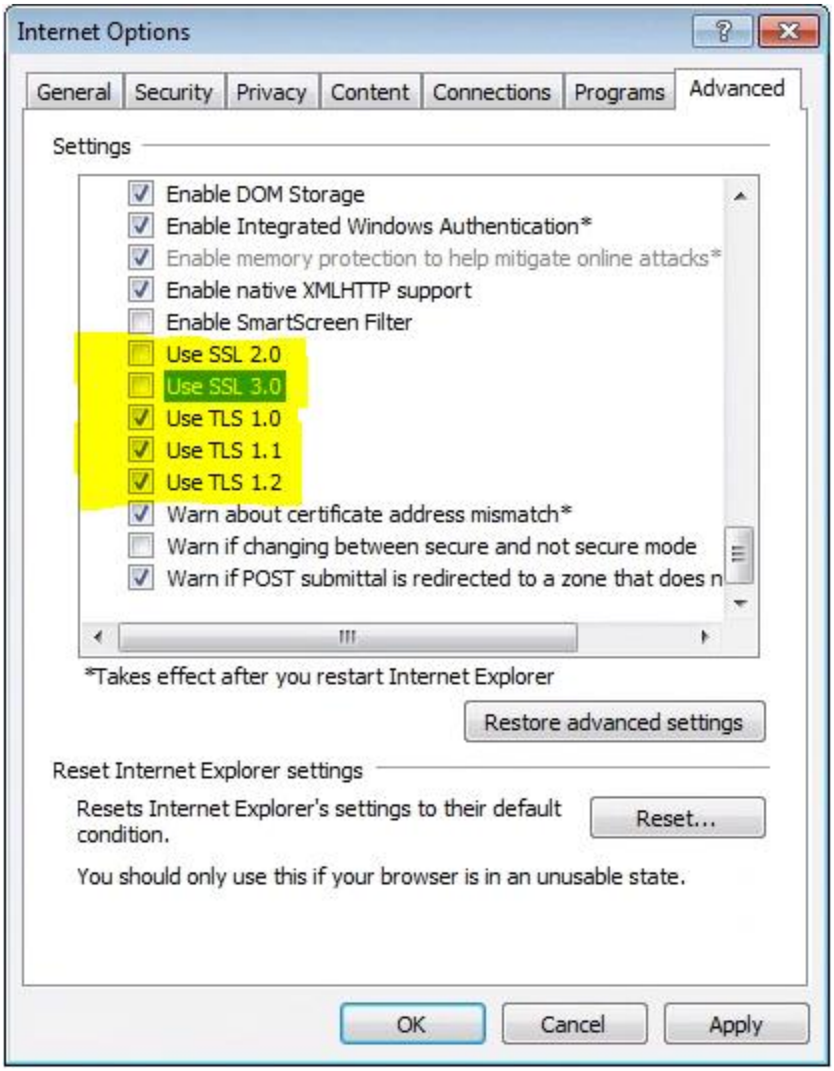
Enabling TLS Protocols in Windows

Not all of Windows operating systems support the latest TLS protocols, or they support the protocols but are turned off by default. The table below lists the operating systems and TLS support.

Windows OS version	SSL 12.0	SSL 3.0	TLS 1.0	TLS 1.1	TLS 1.2	Comments
Windows XP & Windows 2003	✓	✓	✓	X	X	Use FireFox
Windows Vista & Windows Server 2008	✓	✓	✓	X	X	Use FireFox
Windows 7 & Windows Server 2008, R2	✓	✓	✓	✓	✓	Must turn on **
Windows 8 & Windows Server 2012	✓	✓	✓	✓	✓	Must turn on. **
Windows 8.1 & Windows Server 2012 R2	✓	✓	✓	✓	✓	
Windows 10 & Windows Server 2016	✓	✓	✓	✓	✓	

** To enable the protocols, follow these steps:

1. Launch Internet Explorer, navigate to Tools -> Internet Options -> Advanced. Under the Security section, you will see the list of SSL protocols supported by IE.
2. Check TLS 1.1 and TLS 1.2.
3. Click Apply, then click OK to close the dialog.



☑ Enable DOM Storage

☑ Enable Integrated Windows Authentication*

☑ Enable memory protection to help mitigate online attacks*

☑ Enable native XMLHTTP support

☐ Enable SmartScreen Filter

☐ 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 Internet Explorer

Resets Internet Explorer's settings to their default condition.

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

Secure Hash Algorithm

FireLight uses the SHA-1 hashing algorithm to ensure the integrity of generated artifacts within the system. Industry best practices suggest companies leverage the stronger SHA-2 algorithms that are more secure. Insurance Technologies will be transitioning over to the SHA-2 algorithm for the 2.11 release slated for October 2017.

What is SHA and how is it used in FireLight?

Secure Hash Algorithm (SHA) is a family of cryptographic hash functions published by the National Institute of Standards and Technology. The algorithm was designed by the NSA to be part of the Digital Signature Algorithm (DSA) which is a federal information processing standard for digital signatures.

The SHA algorithms takes a source document and generates a one-way hash value representation of the document. The hash value can be used to verify the integrity of the document because a single change in the document will generate a different hash. The hash is also one-way so a user having access to the hash cannot determine the source document.

FireLight uses the algorithm in a two different ways:

1. During the esignature digital signature workflow, SHA-1 hash is used to ensure the integrity of documents generated by the system. A SHA-1 hash of the document is stored or transmitted with the document. The client or receiving system would generate a similar hash of the delivered document and compare it to the FireLight generated hash.
2. To secure passwords by storing the hash of the password instead of the password directly.

What is the change?

Insurance Technologies will be upgrading to use the more secure SHA-2 algorithm. This change will apply to functions within FireLight that are used ensure the integrity of documents, and to securing passwords.

What is the impact?

Any new documents generated from FireLight will utilize the more secure SHA-2 algorithm. The upgrade will not affect existing documents generated in FireLight prior to the upgrade.

The upgrade will enforce the use of SHA-2 to generate hashes of new passwords entered into the system. Passwords in FireLight expire every 90 days. Since a hashed value is “one-way” we cannot convert existing hashed values to SHA-2 so we will instead wait for the passwords to expire to convert the hash to SHA-2. This means we will have SHA-1 stored hashed values for at maximum of 90 days after the upgrade.