

**TLS Upgrade – FAQs**

*** General Questions***

****** [***Technical Questions***](https://letsencrypt.org/docs/faq/#technical)

 ***Browser compatibility***

 ***How to proceed in case of error***

**What is the change?**

Experian Health is requiring an upgrade to ***TLS 1.2*** by October 31, 2017 at 10:00 pm CT.

Experian Health will disable the TLS 1.0 encryption protocol. This phased approach will prevent it from being used to access Experian Health services within inbound and outbound connections.

**Why is Experian Health making this change?**

Experian Health is focused on helping our customers improve their security by using the latest security protocols. On October 31, 2017, Experian Health will require ***TLS 1.2*** and later encryption protocol to maintain the highest security standards and promote the safety of customer data.

Vulnerabilities have been identified therefore we are urging customers to configure their browsers to support ***TLS 1.2*** as soon as possible.

At Experian Health, we take the protection of our customer’s data very seriously. The disablement of TLS 1.0 is being undertaken so we can maintain the highest security standards and promote the safety of your data as well as align with industry-wide best practices.

**What is the impact of this TLS 1.0 and TLS 1.1 disablement?**

The impact of the TLS 1.0 disablement will vary by org, and depends on the ways in which your users connect to the Experian Health service. Key areas of impact include:

 **User browser access** – Browser incompatibility will prevent your internal and external users from accessing your Experian Health org, Communities and Sites. **API integrations** – These integrations will cease to work if they are not compatible with ***TLS 1.2*** or later.

**Partner App/AppExchange Integrations** – Partner App/AppExchange Integrations will cease to work if they are not compatible with ***TLS 1.2*** or later.

**Case submission and management** – Admins using incompatible browsers will be unable to access the Experian Health Help & Training portal, impacting case submission and management.

**What action do I need to take?**

Review how your users and integrations connect to Experian Health and ensure those connections are ready to support ***TLS 1.2*** and later well before October 31, 2017.

Many of our products and developer tools are already compatible with the latest versions of TLS. Customers should start early with their planning and testing to ensure a successful transition to supporting the latest TLS version prior to our enablement of ***TLS 1.2***. Check out the **TLS 1.2 Enablement Readiness Checklist** for best practices on how to prepare for this change.

🞏  Does my browser support TLS 1.2?

|  |  |
| --- | --- |
|  **Operating System** | **Minimum Browser Version** |
| Windows 7/8 | Internet Explorer 10 |
| Windows 10 | Internet Explorer 11Microsoft Edge 12 |
| Windows Server 2008 R2/2012 (or later) | Internet Explorer 10\* |
| Windows Server 2016     | Internet Explorer 11 |
| Apple OS X 10.9 (or later) | Safari 7 |
| Apple iOS6 (or later) | Safari 7 |
| Google Android 5.0 (or later) | Android OS Browser |
| Any  | Google Chrome 38Mozilla Firefox 34 (ERS 31.3) |

 **Note:** Operating Systems and browsers prior to the listed versions will not support TLS 1.2

🞏 Test TLS 1.2 Status: [**https://quickstream.westpac.com.au/quickportal/BrowserTlsVersionView**](https://quickstream.westpac.com.au/quickportal/BrowserTlsVersionView)

🞏 If TLS 1.2 is supported and enabled- You're done!!!

🞏 If TLS 1.2 is not supported or not enabled:

🞏 Determine your browser type and version

🞏 Follow Experian Health FAQ directions on enabling TLS 1.2

🞏 Contact your IT department

 **How do I know if we are ready for this change, how to avoid disruption of service?**

We encourage customers to continue to execute their plans to use ***TLS 1.2*** exclusively. After Experian Health disables TLS 1.0, any inbound connections to or outbound connections from Experian Health will need to use the ***TLS 1.2*** encryption protocol. Your users should not experience an impact accessing Experian Health in your browser(s) unless you are using a non-supported browser or you have disabled the supported encryption protocols in the browser.

**What are the requirements?**

In order to upgrade to ***TLS 1.2***, you must have one of following (or later) versions of the browsers listed:

* Microsoft Internet Explorer 10 (or later) on Windows 7 or later. Also available on Windows Sever 2008 R2 or later.

**Note** Microsoft IE 10 has TLS 1.2 disabled by default.   To enable TLS, use the Advanced Internet Options and apply the TLS 1.2 checkbox.

* Microsoft Edge
* Google Chrome 38 or later on Windows 7 or later. (Also available on Mac OSX 10.9 or later.)
* Google Android 5.0 or later
* Mozilla Firefox 34 (ERS 31.3) or later
* Apple Safari 7 or later (both Desktop and Mobile) on Mac OS X 10.9 and iOS6 or later.

**Browser Requirements**

|  |  |
| --- | --- |
|  **Operating System** | **Minimum Browser Version** |
| Windows 7/8 | Internet Explorer 10 |
| Windows 10 | Internet Explorer 11Microsoft Edge 12 |
| Windows Server 2008 R2/2012 (or later) | Internet Explorer 10\* |
| Windows Server 2016  | Internet Explorer 11 |
| Apple OS X 10.9 (or later) | Safari 7 |
| Apple iOS6 (or later) | Safari 7 |
| Google Android 5.0 (or later) | Android OS Browser |
| Any  | Google Chrome 38Mozilla Firefox 34 (ERS 31.3) |

**Product Requirements**

* IntelliSource/PIC/OneSource: Microsoft .net Version 2.0 Service Pack 2
* eCareNext: Microsoft .net Version 3.5

**Hardware and Operating System Requirements**

* For all products, Microsoft Windows 7 or higher.

 **What's a browser?**

A browser is a software application that lets you visit web pages on the Internet. Popular browsers include Google Chrome, Firefox, Safari, Edge and Internet Explorer.

**Why is my browser information so important?**

Different browsers have different capabilities. And although these differences may seem minor, it’s common for websites to work fine on one browser but poorly on another. The information on this page may help support teams troubleshoot technical issues specific to your browser.

**What browser am I using and what version is my browser?**

All these questions have a quick answer through the [***http://www.whatsmybrowser.org/***](http://www.whatsmybrowser.org/)link, the following scenarios are good examples.



**How do I test my browser compatibility?**

To quickly test your browser compatibility, you can visit the [Browser TLS Version Check](https://quickstream.westpac.com.au/quickportal/BrowserTlsVersionView) page:

[***https://quickstream.westpac.com.au/quickportal/BrowserTlsVersionView***](https://quickstream.westpac.com.au/quickportal/BrowserTlsVersionView)

Which has ***TLS 1.2*** enabled. If you are able to view the site without errors, access to Experian Health via your browser should not be impacted by this change.

 See the following example for a better reference:

**What happens when my browser is not compatible?**

In case your browser is not able to work with the ***TLS 1.2*** enabled protocol, the following Pop-up Message will be displayed within Experian Health products. In order to disable this message, please contact your IT Department.



Internet Explorer 11.0 is preferred as Support for TLS 1.1 and 1.2 is enabled by default, but we will continue to allow IE 8, 9, and 10 as long as ***TLS 1.2*** is enabled.  Please note that Internet Explorer Versions 8, 9 and 10 do not have ***TLS 1.2*** enabled by default and must be configured!

We encourage you to make certain this is communicated to your IT department as soon as possible. Chrome, Firefox, and Safari will run most Passport applications, but not all and therefore not recommended.

The compatibility guide includes details on each browser and version.

**Enabling TLS 1.2 at your web browser**

If you have rights to change your browser settings manually, you may do so by following the below instructions, if not, please contact your IT department or Helpdesk immediately to request their assistance with this change.

Below you will find the different ways to enable the ***TLS 1.2*** protocol for the following browsers:

* Internet Explorer 8
* Internet Explorer 9
* Internet Explorer 10
* Google Chrome
* Mozilla Firefox
* Safari
* Opera

Attached at the end of the document we indicate how to proceed when you experience issues or difficulties with the TLS 1.2 protocol in your browser, so we recommend that you read the table with the compatibility guidelines carefully.



Internet Explorer 8

 **How to Enable TLS 1.2 in the Internet Options of Internet Explorer 8?**

This option works well with one or a small number of computers, particularly if the ***TLS 1.2*** option is not being configured using Active Directory group policies.

In the Tools menu, which is displayed by clicking on the Tools button near the top-right corner of an Internet Explorer 8 window, select the "Internet Options" menu item, as depicted below:

In the Internet Options window that appears, click on the Advanced tab at the top of the window. Scroll down to the end of the list and click the check box next to "Use TLS 1.2”. For additional security, click the check box next to "Use SSL 3.0" if it has a check mark in it to remove the check mark. When complete, the screen should resemble the following, where "Use TLS 1.2" has a check mark in the check box next to it; while "Use SSL 2.0", "Use SSL 3.0" and "Use TLS 1.0" do not have check marks in the check boxes next to them. Press the OK button to save this change.





Internet Explorer 9

**How to Enable TLS 1.2 in the Internet Options of Internet Explorer 9?**

This option works well with one or a small number of computers, particularly if the ***TLS 1.2*** option is not being configured using Active Directory group policies.

In the Tools menu, which is displayed by clicking on the gear icon near the top-right corner of an Internet Explorer 9 window, select the "Internet options" menu item, as depicted below:

In the Internet Options window that appears, click on the Advanced tab at the top of the window. Scroll down to the end of the list and click in the square check box next to "Use TLS 1.2”. For additional security, click in the square check box next to "Use SSL 3.0" if it has a check mark in it to remove the check mark. When complete, the screen should resemble the following, where "Use TLS 1.2” has a check marks in the check box next to it; while "Use SSL 2.0","Use SSL 3.0” do not have check marks in the check boxes next to them. Press the OK button to save this change.



Internet Explorer 10

 **How to TLS 1.2 in the Internet Options of Internet Explorer 10?**

This option works well with one or a small number of computers, particularly if the ***TLS 1.2*** options are not being configured using Active Directory group policies.

In the Tools menu, which is displayed by clicking on the gear icon near the top-right corner of an Internet Explorer 10 window, select the "Internet options" menu item, as depicted below:

In the Internet Options window that appears, click on the Advanced tab at the top of the window. Scroll down to the end of the list and click in the square check the box next to "Use TLS 1.2”. For additional security, click in the square check box next to "Use SSL 3.0" if it has a check mark in it to remove the check mark. When complete, the screen should resemble the following, where "Use TLS 1.2" has a check marks in the check box next to it while "Use SSL 2.0" and "Use SSL 3.0” do not have check marks in the check boxes next to them. Press the OK button to save this change.



Google Chrome

**How to Enable TLS 1.2 in Google Chrome?**

Open Google Chrome

Click Alt F and select Settings

Scroll down and select Show advanced settings...

Scroll down to the Network section and click on Change proxy settings...

Select the Advanced tab

Scroll down to Security category, manually check the option box for Use ***TLS 1.2***



**Mozilla Firefox**

**How to Enable TLS 1.2 in Mozilla Firefox?**

Open Firefox

In the address bar, type about:config and press Enter

In the Search field, enter tls. Find and double-click the entry for security.tls.version.min

Set the integer value to 3 to force protocol of TLS 1.3



Click OK

Close your browser and restart Mozilla Firefox



 **Safari**

**How to Enable TLS 1.2 in Safari?**

To enable TLS 1.2 in Safari, perform the following steps:

There are no options for enabling SSL or TLS protocols.

If you are using Safari version 7 or greater, TLS 1.2 is **automatically enabled.**



 **Opera**

**How to Enable TLS 1.2 in Safari?**

To enable TLS 1.1 and 1.2 in Opera, perform the following steps:

1. Open Opera
2. Click Ctrl+F12.
3. Click on “Security”
4. Click on “Security Protocols…”
5. Locate and check "Use TLS 1.2” to add it.
6. 6. (optional) You may deselect “Use TLS 1.0” if your other financial/secure sites do not require it.
7. Click the "OK" button.
8. Click the "OK" button.

**What should I do if I experience errors?**

If you still experience TLS errors and your Browser is different than Internet Explorer, please refer to the compatibility guidelines below and communicated to your IT department as soon as possible:

|  |  |
| --- | --- |
| **Browser** | **TLS 1.1 or Higher Compatibility Notes** |
| Desktop and mobile IE version 11 | Compatible by default |
| Desktop IE versions 8, 9, and 10  | Capable when run in Windows 7 or newer, but not by default. Windows Vista and older operating systems, such as Windows XP, are not compatible with TLS 1.1 or higher encryption. |
| Desktop IE versions 7 and below | Not compatible with TLS 1.1 or higher encryption. |
| Mobile IE versions 10 and below | Not compatible with TLS 1.1 or higher encryption. |
| Microsoft Edge  | Compatible by default. |
| Google Chrome  | Compatible with the most recent, stable version, regardless of operating system. |
| Google Chrome 38 and higher  | Compatible by default. |
| Google Chrome 22 to 37 | Capable when run in Windows XP SP3, Vista, or newer (desktop), OS X 10.6 (Snow Leopard) or newer (desktop), or Android 2.3 (Gingerbread) or newer (mobile). |
| Google Chrome 21 and below | Not compatible with TLS 1.1 or higher encryption. |
| Desktop Safari v7 and higher OSX10.9  | Compatible by default. |
| Desktop Safari v6 and below for OSX10.8  | Not compatible with TLS 1.1 or higher encryption. |
| Mozilla Firefox  | Compatible with the most recent, stable version, regardless of operating system. |
| Firefox 27 and higher | Compatible by default. |
| Firefox 23 to 26  | Capable, but not by default. |
| Firefox 22 and below | Not compatible with TLS 1.1 or higher encryption. |
| Android 5.0 (Lollipop) and higher | Compatible by default. |
| Android 4.4 (KitKat) to 4.4.4 | Capable, but not by default. |
| Android 4.3 (Jelly Bean) and below | Not compatible with TLS 1.1 or higher encryption. |
| Mobile Safari versions 5 and higher for iOS 5 and higher | Compatible by default. |
| Mobile Safari for iOS 4 and below | Not compatible with TLS 1.1 or higher encryption |