



TLS 1.2 Upgrade Standard - FAQs

Frequently Asked Questions Related to Experian Health's TLS 1.2 Upgrade



TLS 1.2 Upgrade Standard, FAQs – April 26, 2018

The information contained in this document and any attached documents are intended only for the personal and confidential use of the designated user(s). This document contains confidential and privileged information. If the reader of this document is not the intended user (or an agent of the intended user), you are hereby notified that any unauthorized distribution or copying of this document or the information contained in it is strictly prohibited. Experian Health is not responsible for errors or omissions in this technical document.

Copyright © 2018 Experian Health. All rights reserved.

ZZZ

This page intentionally left blank.

TLS 1.2 Upgrade Standard, FAQs - Table of Contents

Immediately Action – White List, TLS 1.2, and PCI Deadlines – Now Approaching	5
White Listing Our Product Domains, URLs, and IP Addresses	5
Financial Products Upgrade Deadline - May 4, 2018.....	5
White List for Financial Products and Payment Safe.....	5
Non-Financial Products Upgrade Deadline - June 30, 2018	6
White List for Medical Necessity	6
Trusted Client Support Sites / IP White List	6
Extended TLS 1.2 Requirement Deadlines (03.23.2018)	7
Security Deadlines and Using the TLS 1.2 Document	7
Product Specific Actions Required.....	7
Medical Necessity.....	7
General TLS 1.2 Upgrade Requirements	8
Experian Health and TLS 1.2 Requirements	8
How Do You Avoid a Disruption of Service?	8
TLS 1.2 Requirements – Frequently Asked Questions.....	8
When is this change?.....	8
Why is Experian Health making this change?.....	8
TLS 1.2 – Requirements and Action Items.....	9
What is the Impact of Disabling TLS 1.0 and TLS 1.1?	9
Hardware and Operating System Requirements	9
Operating System and Internet Browser Access.....	9
API Integrations (Products such as eCare NEXT Bar, IntelliSource, Legacy Medical Necessity, etc.)	9
Partner App/AppExchange Integrations.....	9
Case Submission and Management	9
Does the NEXT Bar and IntelliSource (PIC) Update to TLS 1.2 Automatically?	10
TLS 1.2 – Operating System and Browser Requirements	11
What is an Internet Browser?	11
Step 1: TLS 1.2 Operating System and Internet Browser Checklist.....	11
What are the Internet Browser Requirements?.....	12
Why is my browser information so important?	12
Step 2: TLS 1.2 Internet Browser – Determine the Browser You are Using	13
What Internet Browser Do I Have?	13
Test Your Internet Browsers Compatibility?	13
What Happens When the Internet Browser Is NOT Compatible?	14
Step 3: Enabling TLS 1.2 on Your Internet Browser	15
Operating System and Browser Compatibility Issues and Difficulties	15
To Enable TLS 1.2 – Internet Explorer 8.....	16
To Enable TLS 1.2 – Internet Explorer 9.....	17
To Enable TLS 1.2 – Internet Explorer 10.....	18
To Enable TLS 1.2 – Google Chrome.....	19
To Enable TLS 1.2 – Mozilla Firefox	20
To Enable TLS 1.2 – Safari	20
To Enable TLS 1.2 – Opera.....	20
TLS 1.2 – Operating System and Browser Compatibility Issues	21
TLS 1.2 – API Requirements, Windows .NET 4.6.2 Framework	22
Step 1: Download Installation, Windows .NET 4.6.2 Framework	22
Use Link to Download and Install Microsoft Windows .NET 4.6.2 Framework	22
Hardware and Operating System Requirements	22
Experian Health’s Product Requirements	22
TLS 1.2 – Interface Requirements – NEXT Bar and IntelliSource (PIC)	23
TLS 1.2 Compliant Versions of the NEXT Bar and IntelliSource (PIC).....	23
How Can You Determine if a Staff Member is Using the NEXT Bar?	23
Step 1: Determine Your Product Interface – NEXT Bar and IntelliSource (PIC)	24
NEXT Bar – Click Once vs. MSI Version	24
Click Once.....	24

MSI	24
IntelliSource (PIC) – Click Once vs. MSI Version	25
Click Once	25
MSI	25
Step 2: Use Links to Update Your NEXT Bar or IntelliSource (PIC) Interface	26
Experian Health Product Requirements - Microsoft .NET Version 4.6.2	26
Link: NEXT Bar MSI Installer: – For Click Once Clients	26
Link: NEXT Bar Click Once – For Click Once Clients	26
Link: NEXT Bar MSI Installer with Log In Prompt: – For MSI Clients	26
Link: Passport IntelliSource Client (PIC) – For Click Once Clients	26
Link: Passport IntelliSource Client (PIC) – For MSI Clients	26
NEXT Bar or IntelliSource (PIC) Issues and Troubleshooting	27
NEXT Bar – Freezing or Disappearing	27
NEXT Bar – How to Use the Click Once Cleaner (New Link)	28
Instructions for using the Cleaner:	28
NEXT Bar – To Re-Install the Old Version	28
Old Link: NEXT Bar MSI Installer: – For Click Once Clients	28
Old Link: NEXT Bar Click Once – For Click Once Clients	28
Old Link: NEXT Bar MSI Installer with Log In Prompt: – For MSI Clients	28
Old Link: Passport IntelliSource Client (PIC) – For Click Once Clients	28
Old Link: Passport IntelliSource Client (PIC) – For MSI Clients	28
General FAQs	29
I Noticed the Wrong Account Manager Listed on My Account?	29
We are in the Middle of Our Implementation Process?	29
Is it Okay To Provide User Information to During the Upgrade Process?	29
Is there a Difference Between the “eCareNEXT Bar” and the “NEXT Bar?”	29
If the Test User’s Web Browser is Verified for TLS 1.2 Compliance, Are Other Users Good to Go?	29
Who are what is iPeople? And Who Do We Contact to Update Our Scripting Process?	30
Is the Client/User Report Specifically to the NEXT Bar and HIS System Usage?	30
Closing – Maintaining the Highest Security Standards	30
What You Should Know	30

Immediately Action – White List, TLS 1.2, and PCI Deadlines – Now Approaching

White Listing Our Product Domains, URLs, and IP Addresses

In the event your location cannot meet these deadlines, please immediately reach out to us at customer.support@experianhealth.com so that we can audit the progress of your required upgrades.

Due to PCI Compliance and TLS 1.2 Security Requirements, clients or end users who process payments using any of our Financial Products (PaymentSafe, Link2Gov or L2G, Concord/First Data, Patient Self-Service, Cash Tracking) must take the following action.

Financial Products Upgrade Deadline - May 4, 2018

Please inform and communicate with your IT Staff and/or Network Administrators, to ensure that each of the following Domains and IP addresses are included and/or added in your Network Configuration and “White Listed” for any of your network proxy servers and firewalls. To avoid any service disruption and/or end-user access, please complete this action prior to May 4, 2018.

White List for Financial Products and Payment Safe

If your project includes our PaymentSafe module, and other Financial Products, also “White List”: the following Domains and IP addresses. Our Financial Products include PaymentSafe, Link2Gov or L2G, Concord/First Data, Patient Self-Service, and Cash Tracking

- paymentsafe.experianhealth.com

199.96.232.175	199.96.233.175
----------------	----------------

- collections.ecarenext.com

199.96.232.176	199.96.233.176
----------------	----------------

Non-Financial Products Upgrade Deadline - June 30, 2018

Clients Who Use Our Non-Financial Products

Must Complete Their Upgrades by: June 30, 2018.

White List for Medical Necessity

If your project includes our Medical Necessity module, also “White Listed”: the following URLs and Domains in your firewall.

- <https://hworks.info>
- <https://prod.hworks.com>

Trusted Client Support Sites / IP White List

For the best communication experience with our client services teams the following IP addresses should also be included in your “White List”. Inclusion of these IP address ranges are specific to our CRM usage, email, and other communications between you and our Client Support Systems.

13.108.238.128	13.108.238.159
13.108.254.128	13.108.254.159
96.43.144.64	96.43.144.78
96.43.147.64	96.43.147.78
96.43.148.64	96.43.148.78
96.43.151.64	96.43.151.78
136.146.128.64	136.146.128.78
136.147.46.176	136.147.46.206
136.146.208.16	136.146.208.30
136.146.210.16	136.146.210.30
136.147.62.176	136.147.62.206
136.147.46.208	136.147.46.238
136.147.62.208	136.147.62.238
204.14.232.64	204.14.232.78

Extended TLS 1.2 Requirement Deadlines (03.23.2018)

Due to PCI Compliance Requirements, Clients who use our Financial Products (PaymentSafe, Link2Gov or L2G, Concord/First Data, Patient Self-Service, Cash Tracking) Must Have TLS 1.2 Enabled by Friday, May 4, 2018 to Prevent Service Disruption. Clients who use our Non-Financial Products must complete their upgrades by June 30, 2018. In the event your location cannot meet these deadlines, please immediately reach out to us at customer.support@experianhealth.com so that we can audit the progress of your upgrade.

Security Deadlines and Using the TLS 1.2 Document

This document contains FAQs, Readiness Checklist, Compatibility, and Product Testing for the TLS 1.2 security upgrade. In addition to TLS 1.2 enabled Internet Browsers, eCare NEXT Bar (Click-Once, MSI, IPS), IntelliSource (PIC), and Medical Necessity clients must upgrade their applications.

- If you have our Financial Products – Your Deadline is May 4, 2018
To upgrade your Internet Browser, NEXT Bar, and IntelliSource (PIC).
- If you don't have our Financial Products – Your Deadline is June 30, 2018
To upgrade Internet Browser, NEXT Bar, and IntelliSource (PIC).

Product Specific Actions Required

eCare NEXT Bar (Click-Once, MSI, IPS) and IntelliSource (PIC) clients must upgrade their applications. Instructions for testing can be found in this document.

Medical Necessity

Requirements and instructions to upgrade Medical Necessity Thin Client are available for download on our product dashboard. This is only for clients who use the Legacy Order Checker application (a/k/a Healthworks and IntelliSource Medical Necessity). This update does not apply to clients who have Order Checker within the eCare NEXT platform.

General TLS 1.2 Upgrade Requirements

Experian Health and TLS 1.2 Requirements

Experian Health is focused on helping our customers improve their security by using the latest security protocols. At Experian Health, we take the protection of our customer's data very seriously. The disablement of TLS 1.0 and TLS 1.1 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.

Clients will be required to perform the necessary web browser, software specific updates, and .NET upgrades before May 4, 2018. Your users should not experience any impact accessing Experian Health, unless you are using a non-supported browser, have disabled the supported encryption protocols in your browser, or have not upgraded to the Microsoft .NET 4.6.2 framework as required for the new NEXT Bar, PIC, and Smart Agent deployments.

Note: To be compliant with TLS 1.2 Standards, the newest version of the NEXT Bar requires the Microsoft .NET 4.6.2 Framework or higher. Microsoft .NET Frameworks prior to version 4.6.2 are Not Supported.

How Do You Avoid a 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 and TLS 1.1, 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.

TLS 1.2 Requirements – Frequently Asked Questions

When is this change?

Experian Health is already in the process of enabling the TLS 1.2 upgrade, which is scheduled for completion by May 4, 2018 at 10:00p.m. CT. This phased approach will prevent it from being used to access Experian Health services for all inbound and outbound connections. After May 4, 2018, Experian Health will disable the TLS 1.0 and TLS 1.1 encryption protocols.

Why is Experian Health making this change?

Since the introduction of TLS 1.0 and TLS 1.1, vulnerabilities have been identified in these older encryption protocols. To maintain the highest security standards and industry-wide best practices, Experian Health will require TLS 1.2 and later encryption protocol on May 4, 2018.

TLS 1.2 – Requirements and Action Items

Prior to production use, clients will be required to perform the necessary web browser, software specific updates, and .NET upgrades before 04/02/2018. Your users should not experience an impact accessing Experian Health in your browser(s) unless you are using a non-supported browser, have disabled the supported encryption protocols in the browser or have not upgraded to minimum .NET 4.6.2 framework required for new NEXT Bar, PIC and Smart Agent deployments.

- Applications that communicate with the Experian Health network must use TLS 1.2.

What is the Impact of Disabling TLS 1.0 and TLS 1.1?

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:

Hardware and Operating System Requirements

For all products, Microsoft Windows 7 or Higher.

Operating System and Internet Browser Access

Older Operating Systems and Internet Browsers may not support TLS 1.2. Any incompatibility may prevent your internal and external users from accessing your Experian Health's Products and Services, Communities, and Other Sites.

API Integrations (Products such as eCare NEXT Bar, IntelliSource, Legacy Medical Necessity, etc.)

API Integrations will stop working if they are not compatible or upgraded with the TLS 1.2 or later.

Important: *Depending on the Experian Health products you use, the Authentication Process (Username and Password) will occur either within your Internet Browser (for the OneSource Web Interface) or within the eCare NEXT Bar and IntelliSource (PIC). In other words, sign-on traffic from the NEXT Bar to Experian Health requires TLS 1.2 encryption when logging in.*

- Both the User's Internet Browser and their PIC/NEXT Bar must be upgraded to TLS 1.2 compliant versions. In most cases, there are only two applications in play, your Internet Browser and the PIC (Passport IntelliSource Client) or NEXT Bar. Both run on the User's Desktop or Citrix environment.

Partner App/AppExchange Integrations

Partner App/AppExchange Integrations will stop working if 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, Case Submission and Management Tools.

Does the NEXT Bar and IntelliSource (PIC) Update to TLS 1.2 Automatically?

The TLS 1.2 upgrade required us to use a new URL to publish the new TLS 1.2 Compliant NEXT Bar and IntelliSource (PIC). Because of this, the old version will not automatically update to the newest TLS 1.2 compliant version.

The reason for this, is that in many cases, a client's machine, would not have the most recent Microsoft .NET version of 4.6.2 installed. Hence, if an automated upgrade occurred, the new TLS 1.2 NEXT Bar would not be capable of running.

Once you have installed the new TLS 1.2 NEXT Bar, the Click Once versions will again automatically update as we continue to publish future deployments to the new URL in the future. Using this document, you can determine which version of the NEXT Bar or IntelliSource (PIC) you are using, as well as the new URLs you can use to download the latest TLS 1.2 product.

IntelliSource (PIC) assembly versions will have 2017 in the date. NEXT Bar assemblies will have 2018 in the date, with the most recent release being version 2018.03.14. Any versions that have dates prior to those are not TLS 1.2 compliant.

TLS 1.2 – Operating System and Browser Requirements

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 May 4, 2018.

What is an Internet 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.

Step 1: TLS 1.2 Operating System and Internet Browser Checklist

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**. Use the included checklists 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 11 Microsoft 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 38 Mozilla 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>
- ☐ 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 Directions on Enabling TLS 1.2.
 - ☐ Contact your IT Department.

What are the Internet Browser Requirements?

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 Server 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 with 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.

Operating System	Minimum Browser Version
Windows 7/8	Internet Explorer 10
Windows 10	Internet Explorer 11 Microsoft 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 38 Mozilla Firefox 34 (ERS 31.3)

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.

Step 2: TLS 1.2 Internet Browser – Determine the Browser You are Using

What Internet Browser Do I Have?

By using the link below, you can quickly learn how your Internet Browser is configured. You may quickly answer all the following questions by using this link, and by reviewing the scenarios and examples on the following pages.

<http://www.whatsmybrowser.org/>

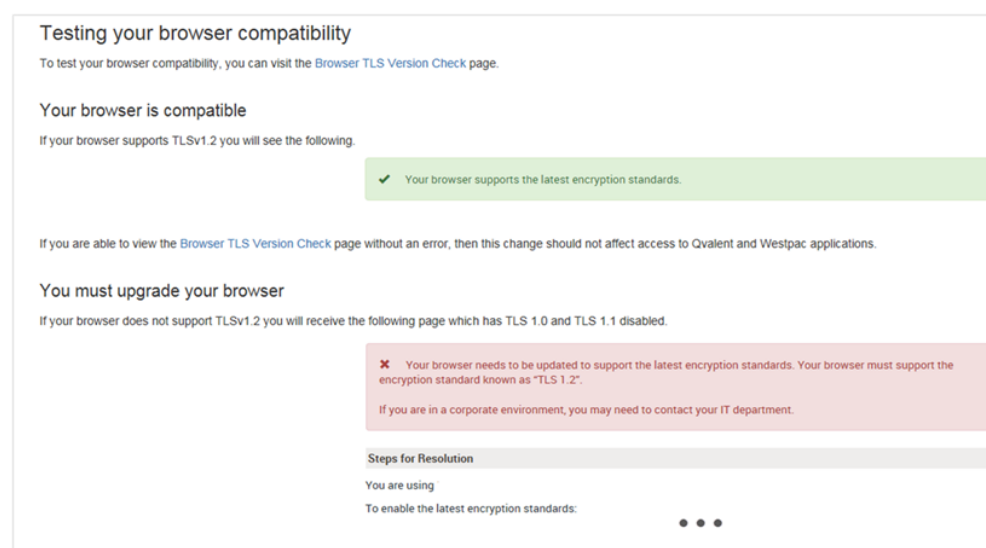


Test Your Internet Browsers Compatibility?

To quickly test your browser compatibility, you can visit the Browser TLS Version Check page:

<https://quickstream.westpac.com.au/quickportal/BrowserTlsVersionView>

Which has **TLS 1.2** enabled. If you can view this 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 the Internet Browser Is NOT Compatible?

In case your browser is not able to work with the **TLS 1.2** enabled protocol, a Pop-up Message similar to that shown below will be displayed within your Experian Health products.

For you to disable this message, please contact your IT Department.

Your browser is using TLS 1.1. You need to upgrade!

TLS 1.1 is an outdated protocol and must be upgraded to 1.2 for improved protection. If you cannot upgrade Internet Explorer to version 11, please enable TLS 1.2 on your Internet Explorer 8, 9 or 10 browsers. It can be configured by clicking on IE Setting, Internet Options, Advanced, and unchecking TLS 1.0 and TLS 1.1 and checking TLS 1.2. We will not allow browsers defaulted to TLS 1.0 or 1.1 to access our products after 3/31/2018.

If you do not have administrative rights to make this change, please contact your IT department or Helpdesk to request their assistance.

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 when **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.

Step 3: Enabling TLS 1.2 on Your Internet 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.

On the following pages you will find instructions 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

Operating System and Browser Compatibility Issues and Difficulties

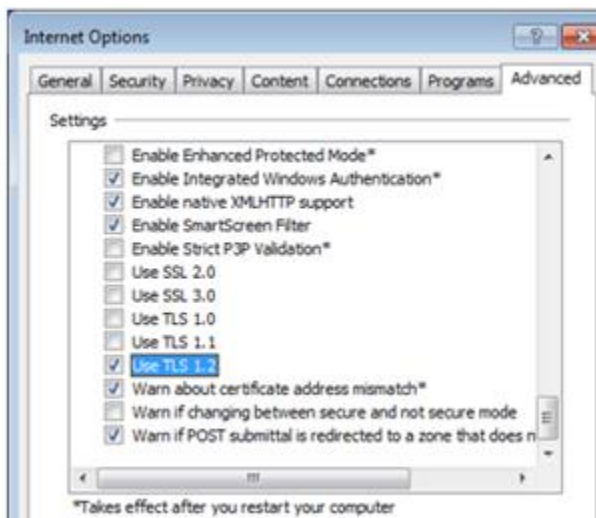
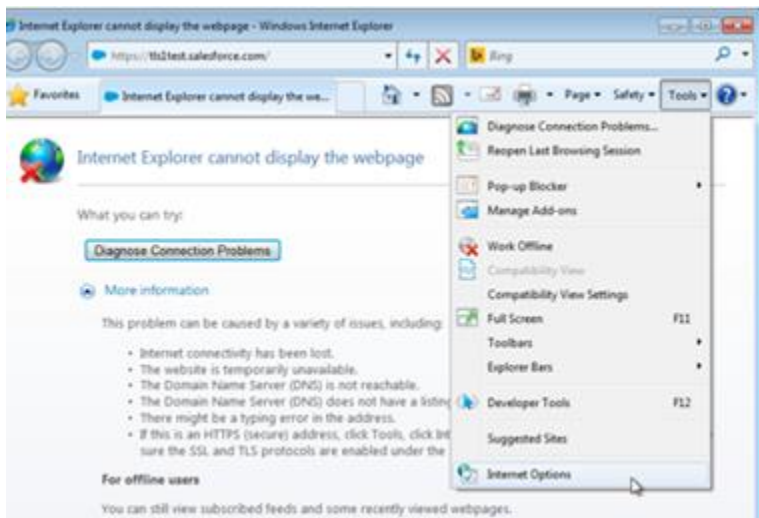
Attached at the end of this section, we indicate how to proceed when you experience compatibility issues or difficulties with the TLS 1.2 protocol in your browser. We recommend that you read the table with the compatibility guidelines carefully and as necessary, consult with your IT staff.

To Enable TLS 1.2 – 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. From 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; and 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.

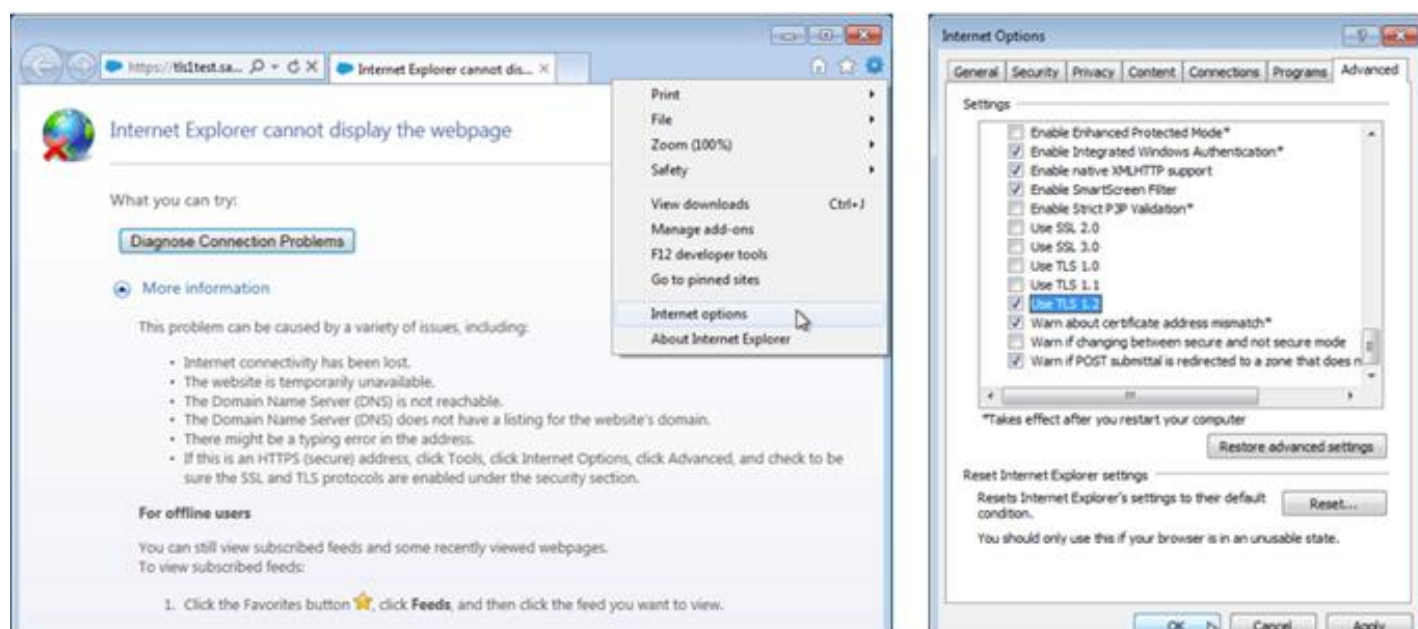


To Enable TLS 1.2 – Internet Explorer 9



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.

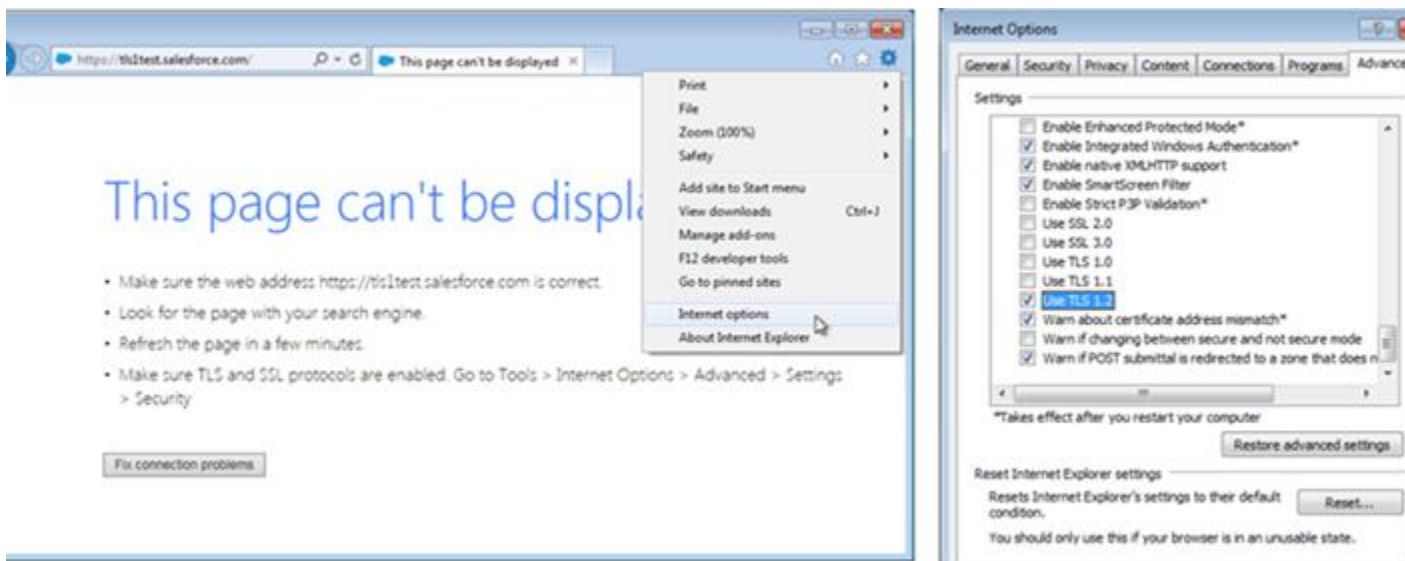


To Enable TLS 1.2 – Internet Explorer 10



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.



To Enable TLS 1.2 – Google Chrome



Open Google Chrome

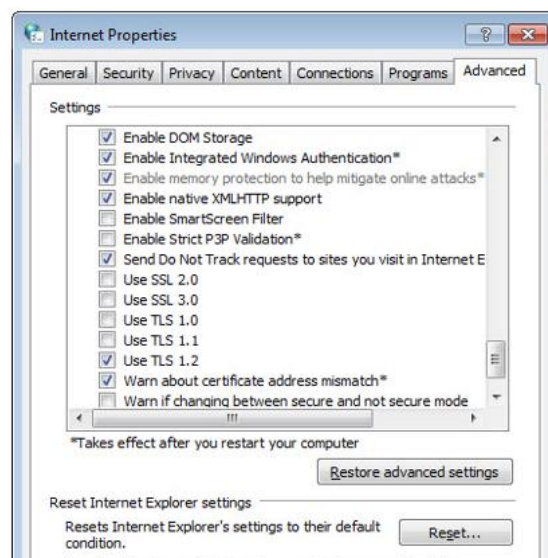
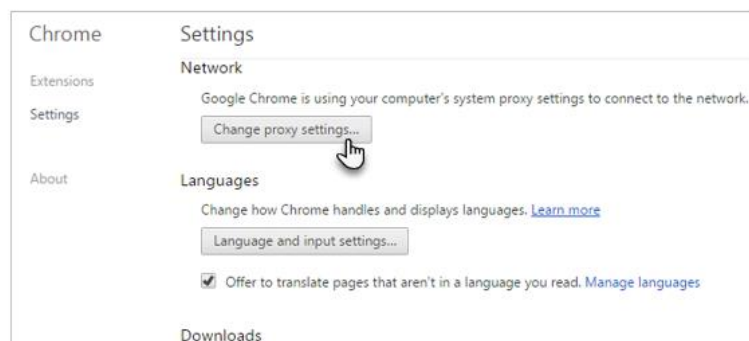
Click Alt F and select Settings

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



To Enable TLS 1.2 – 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

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.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	1
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

To Enable TLS 1.2 – Safari



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.

To Enable TLS 1.2 – Opera



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

Open Opera. Click Ctrl+F12.

Click on “Security.” Click on “Security Protocols...”

Locate and check “Use TLS 1.2” to add it.

(optional) You may deselect “Use TLS 1.0” if your other financial/secure sites do not require it.

Click the “OK” button. And again, click the “OK” button.

TLS 1.2 – Operating System and Browser Compatibility Issues

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

TLS 1.2 – API Requirements, Windows .NET 4.6.2 Framework

Prior to upgrading your client interfaces, it will be necessary for you to download and install the Windows .NET 4.6.2 Framework.

Step 1: Download Installation, Windows .NET 4.6.2 Framework

Your PC will be checked for this upgrade during the installation processes described on the following pages. Any Windows .NET version less than 4.6.2 will first require an upgrade.

Note: *To be compliant with TLS 1.2 Standards, the newest version of the NEXT Bar requires the Microsoft .NET 4.6.2 Framework or higher. Microsoft .NET Frameworks prior to version 4.6.2 are Not Supported.*

Use Link to Download and Install Microsoft Windows .NET 4.6.2 Framework

Use the following link to download and install the Windows .NET Framework.
Once installed, continue to update your Experian Health client interface.

<https://www.microsoft.com/en-us/download/details.aspx?id=53344>

Hardware and Operating System Requirements

For All Products, Microsoft Windows 7 or higher.

Experian Health's Product Requirements

- ☐ IntelliSource/PIC/OneSource: Microsoft .NET Version 4.6.2
- ☐ eCare NEXT: Microsoft .NET Version 4.6.2 Required.

TLS 1.2 – Interface Requirements – NEXT Bar and IntelliSource (PIC)

New URLs have been used to publish the newest TLS 1.2 Compliant NEXT Bar and IntelliSource (PIC). This was done to prevent older software versions from acquiring automatic updates. Because of this, older products will not automatically update to the newest TLS 1.2 Compliant version. In other words, if the automatic update (by the older version) occurred prior to the installation of Microsoft .NET 4.6.2, then the computer will not run the newly installed TLS 1.2 Compliant version.

Once you have installed the newest TLS 1.2 Compliant NEXT Bar, the Click Once versions will again automatically update, and future deployments will be published to new URL.

TLS 1.2 Compliant Versions of the NEXT Bar and IntelliSource (PIC)

The TLS 1.2 Compliant NEXT Bar will have 2018 in the date, the most recent release being version 2018.03.14. Any NEXT Bar versions containing prior dates are not TLS 1.2 compliant. Versions of the IntelliSource (PIC) assembly will have 2017 in the date.

How Can You Determine if a Staff Member is Using the NEXT Bar?




You can determine who is using the NEXT Bar by logging into the Self-Service Portal. Then, click Online Reports, and choose the report named “Users NEXT Bar Info.” This report provides the User Name, Login, Version, Login Type, Login Date, and Form version. If the report is blank, users are not logging into the NEXT Bar.

Step 1: Determine Your Product Interface – NEXT Bar and IntelliSource (PIC)

Using the following descriptions, determine which product interface of the NEXT Bar or IntelliSource (PIC) you are using.

NEXT Bar – Click Once vs. MSI Version

To determine if you are currently using the Click Once or MSI version of the NEXT Bar, check your Control Panel.


- ☐ The Click Once version will show the default application icon .
- ☐ The MSI will show either the old Passport Logo, () or the New Experian Health () Logo.

Optionally, you may look to see where the NEXT Bar application was installed to determine whether the MSI or Click Once version being utilized

Click Once

The Click Once installs to:


C:\Users\“your.user.name”\AppData\Local\Apps\2.0\4AQEZ8JO.EYH\CRQVHK08.OLY\next..tion_8b7fbb6f5f761aa_07e1.0002_4de095302d592fa3

 NEXT Bar	Passport Health Communicatio...	12/4/2017	2017.2.3.1
--	---------------------------------	-----------	------------

MSI




By default, the MSI will be installed to the path:

C:\Program Files (x86)\Passport Health Communications, Inc\NEXT Bar\.

 NEXT Bar	Passport Health Communicatio...	12/4/2017	77.6 MB 02.03.2017
--	---------------------------------	-----------	--------------------

IntelliSource (PIC) – Click Once vs. MSI Version

To determine if you are currently using the Click Once or MSI version of the IntelliSource (PIC), check your Control Panel.

- ☐ The Click Once version will show the default application icon .
- ☐ The MSI will show either the old Passport Logo, () or the New Experian Health () Logo.

Optionally, you may look to see where the IntelliSource (PIC) application was installed to determine whether the MSI or Click Once version being utilized


Click Once

The Click Once Installs to:

C:\Users\“your.user.name”\AppData\Local\Apps\2.0\4AQEZ8JO.EYH\CRQVHK08.OLY\pass..tion_a171c8497eb90460_0009.0008_20d1f4c1ba8f1c33.

Note: *There is no change between the old and new Click Once versions within the Control panel.*

Old:

 Passport IntelliSource Client	Passport Health Communicatio...	12/4/2017	9.8.24.0
---	---------------------------------	-----------	----------

New:


 Passport IntelliSource Client	Passport Health Communicatio...	12/4/2017	2017.11.16.0
---	---------------------------------	-----------	--------------

MSI


By default, the MSI will be installed to the path:

C:\Program Files (x86)\Passport Health Communications\Passport IntelliSource Client.

Old:

 Passport IntelliSource Client	Passport Health Communicatio...	12/4/2017	397 KB	11.03.22
---	---------------------------------	-----------	--------	----------

New:

 Passport IntelliSource Client	Passport Health Communicatio...	12/4/2017	465 KB	11.16.2017
---	---------------------------------	-----------	--------	------------

Step 2: Use Links to Update Your NEXT Bar or IntelliSource (PIC) Interface

Make certain you have rights to make updates to your PC. If not, ask your helpdesk for assistance loading. In subsequent sessions, always accept the newest NEXT Bar or IntelliSource (PIC) updates.

Note: To be compliant with TLS 1.2 Standards, the newest version of the NEXT Bar requires the Microsoft .NET 4.6.2 Framework or higher. Microsoft .NET Frameworks prior to version 4.6.2 are Not Supported.

- MSIs will direct the user to the proper website for download and installation of the new framework. Once upgraded, the Experian installation will resume.
- The new Windows .NET Framework is packaged with the Click Once version. If needed, it will be installed during the Experian application installation.

Experian Health Product Requirements - Microsoft .NET Version 4.6.2

During installation from any of the **new** URLs, the user's PC is checked for the existing .NET Framework version. Anything less than 4.6.2 will need to be upgraded.

- ☐ TLS 1.2 – Link to [Download and Install Microsoft Windows .NET 4.6.2 Framework](#)
- ☐ eCare NEXT – Microsoft .NET Version 4.6.2
- ☐ OneSource/IntelliSource (PIC) – Microsoft .NET Version 4.6.

Link: NEXT Bar MSI Installer: – For Click Once Clients

New:

https://onesource.passporthealth.com/members/software/next_bar_x86_v2/MSI_ClickOnce_Installer/NEXT_Bar_ClickOnce_Installer_Setup.msi

Link: NEXT Bar Click Once – For Click Once Clients

New:

https://onesource.passporthealth.com/members/software/next_bar_x86_v2/publish.htm

Link: NEXT Bar MSI Installer with Log In Prompt: – For MSI Clients

New:

https://onesource.passporthealth.com/members/software/next_bar_x86_v2/MSI_LoginPrompt/PHC.NextBar.Client.Setup.msi

Link: Passport IntelliSource Client (PIC) – For Click Once Clients

New:

https://onesource.passporthealth.com/members/software/PassportIntelliSourceClient_v2/publish.htm

Link: Passport IntelliSource Client (PIC) – For MSI Clients

New:

https://onesource.passporthealth.com/members/software/PassportIntelliSourceClient_v2/MSI/PassportIntelliSourceClient.msi

NEXT Bar or IntelliSource (PIC) Issues and Troubleshooting

If you still experience TLS errors with your NEXT Bar or IntelliSource (PIC) Interface, please refer to the compatibility guidelines below and contact your IT department as soon as possible.

1. Make certain you have rights to make updates to your PC. If not, ask your helpdesk for assistance loading.
2. In subsequent sessions, always accept the newest NEXT Bar updates.
 - MSIs will direct the user to the proper website for download and installation of the new framework. Once upgraded, the Experian installation will resume.
 - The new .NET Framework is packaged with Click Once versions. If needed, it will be installed during the Experian application installation.

NEXT Bar – Freezing or Disappearing

If the NEXT Bar is freezing or disappearing, use these steps to resolve the issue.

If the issue is webpage related (missing chevrons, links in work queues, radio buttons missing, etc.), take the following steps:

- Clear cookies
- Delete temp files and history
- Change browser settings to “check for new versions of stored pages”
- Log out completely/reboot PC and re-launch Bar.

If that does not resolve the problem, you should try the following:

- Go to Start/Control Panel/Programs/Programs and Features
- Select programs to uninstall or change
- Choose the most recent Microsoft.NET Framework (should be at least 3.0) program. When chosen, an Uninstall/Change link should appear just above the column headings.
- Click Uninstall/Change.
- A Pop-up should appear that gives you the option of Repair or Remove.
- Click Repair and Next until finished.
- Reboot.

If you continue to have NEXT Bar issues, someone with admin rights to the PC can right-click on the NEXT Bar, choose about, click on Open Error Log Folder, choose a file from the day the error occurred, and forward to our customer support team.

NEXT Bar – How to Use the Click Once Cleaner (New Link)

http://onesource.passporthealth.com/members/software/NEXT_Bar_x86_v2/MSI_ClickOnce_Cleaner/NEXT_Bar_ClickOnce_Cleaner_Setup.msi

Instructions for using the Cleaner:

1. Uninstall the NEXT Bar
2. Reboot PC
3. Run the Click Once Cleaner
4. Re-Install the NEXT Bar (Also See, To Re-Install the Old Version)
5. Run Application

NEXT Bar – To Re-Install the Old Version

If necessary, use the Click Once Cleaner as described above. Then, use the following links to revert back to the older version of your NEXT Bar interface.

Old Link: NEXT Bar MSI Installer: – For Click Once Clients

https://onesource.passporthealth.com/members/software/next_bar_x86/MSI_ClickOnce_Installer/NEXT_Bar_ClickOnce_Installer_Setup.msi

Old Link: NEXT Bar Click Once – For Click Once Clients

https://onesource.passporthealth.com/members/software/next_bar_x86/publish.htm

Old Link: NEXT Bar MSI Installer with Log In Prompt: – For MSI Clients

https://onesource.passporthealth.com/members/software/next_bar_x86/MSI_LoginPrompt/PHC.NextBar_Client.Setup.msi

Old Link: Passport IntelliSource Client (PIC) – For Click Once Clients

<https://onesource.passporthealth.com/members/software/PassportIntelliSourceClient/publish.htm>

Old Link: Passport IntelliSource Client (PIC) – For MSI Clients

https://onesource.passporthealth.com/members/software/PassportIntelliSourceClient_v2/MSI/PassportIntelliSourceClient.msi

General FAQs

I Noticed the Wrong Account Manager Listed on My Account?

How Did That Happen? What Should I do? This usually is human error. Please let us know and we will update your account.

We are in the Middle of Our Implementation Process?

Who Provide the Requirements? The Implementation team is aware of the TLS 1.2 Requirements and Compliance Deadlines for the NEXT Bar /PIC requirements and are communicating with the clients they are implementing.

Is it Okay To Provide User Information to During the Upgrade Process?

Always treat user information with care. Do not forward entire documents, list, or attachments. When interacting with others during this upgrade process, exercise extreme caution, if you need to copy and paste, or when electronically communicating specific user information.

Is there a Difference Between the "eCareNEXT Bar" and the "NEXT Bar?"

Sometimes I notice a usage report that shows the NEXT Bar as the cause of an issue. This isn't the same as eCareNEXT, right? Correct. This is just indicating the NEXT Bar integration that supports the scripting process used by your HIS platform.

If the Test User's Web Browser is Verified for TLS 1.2 Compliance, Are Other Users Good to Go?

Not necessarily. Staff members can quickly test their browser compatibility, by visiting the Browser TLS Version Check page.

<https://quickstream.westpac.com.au/quickportal/BrowserTlsVersionView>

If you can view this site without errors, access to Experian Health via your browser should not be impacted by this change. When checking a user's Internet Browser, you should receive this message:

"Your Browser Supports the Latest Encryption Standards."

Only then, can you confirm that a user's browser supports the TLS 1.2 upgrade. Applications that communicate with the Experian Health network must use TLS 1.2. In most cases, there are only two applications in play. Both run on the user's desktop or within the Citrix environment. The first application is the Internet Browser and the second application is the IntelliSource (PIC) or NEXT Bar. Both the user's browser and their PIC or NEXT Bar must be upgraded to TLS 1.2 compliant versions.

Who are what is iPeople? And Who Do We Contact to Update Our Scripting Process?

Experian Health have contracted with iPeople to work with our Scripting team for those clients who use iPeople Integration. iPeople will reach out and contact you directly via email. Your Account Manager will also be informed when you are contacted. You do not need to contact iPeople. iPeople is responsible for coordinating the scripting update with our clients.

Is the Client/User Report Specifically to the NEXT Bar and HIS System Usage?

Yes. Since the eCareNEXT Platform is typically used in conjunction with the web browser, those user logins will not be included. In some cases, a HIS user should not be using the NEXT Bar.

Closing – Maintaining the Highest Security Standards

We need to ensure that all TLS 1.2 requirements are met by May 4, 2018. The disablement of TLS 1.0 and TLS 1.1 is being undertaken so we can maintain the highest security standards and promote the safety of our client's data as well as align with industry-wide best practices – like PCI DSS. This phased approach will prevent older encryption protocols from being used to access Experian Health services within inbound and outbound connections.

For those who are not familiar with PCI DSS, Payment Card Industry Data Security Standard - Experian Health has met the requirements of the Payment Card Industry Data Security Standard (PCI DSS) as a Level One Service Provider. Among many requirements, this process includes ongoing third-party security audits, penetration testing, thorough policies and procedures, and rigorous software testing standards. This certification is specific to our financial product suite.

What You Should Know

We are tracking the clients who currently do not meet the TLS 1.2 requirements. Stay in contact with your dedicated Account Manager to discuss the TLS 1.2 requirements and your timeline to implement these updates.