Westpac Quickstream and WIBS

Disabling TLS v1.0 & TLS v1.1

Date	Description
9/10/15	Initial Version
19/10/15	Reviewed
5/11/15	Updated
1/12/15	Updated
7/12/15	Revised

1 Disabling the TLSv1.0 & TLSv1.1 protocol

1.1 Who might this affect?

Any customer who sends data to or accesses Qvalent websites. This includes, but is not limited to the following Qvalent URL's via HTTPS:

- **ccapi.qvalent.com – credit card API**
- **ws.qvalent.com – token requests**
- **ssiw.qvalent.com – WIBS file transfers via HTTPS or SOAP**
- **quickstream.westpac.com.au – web browser access**
- **www.batchadvantage.qvalent.com – web browser access**
- **pnpnet.qvalent.com – web browser access**

1.2 What is SSL and TLS

Secure Sockets Layer (SSL) and Transport Layer Security (TLS) are cryptographic protocols used to provide secure communications over the internet. One of these protocols is used in all HTTPS communications between system to system or browser to system on the internet. TLSv1.0 was released in 1996, TLSv1.1 in 1999 and the current version, TLSv1.2 was released in 2008.

1.3 Why is TLSv1.0 & TLSv1.1 being disabled?

The PCI council have deemed SSLv3 and early TLSv1.0 are no longer considered strong cryptography and cannot be used as a security control after 30th June, 2016. Any organisation that has TLSv1.0 enabled after this date will lose its PCI-DSS compliance.

For full details from the PCI council please refer to:

https://www.pcisecuritystandards.org/documents/Migrating_from_SSL_Early_TLS_Information_Supplement_v1.pdf

1.4 When will TLSv1.0 & TLSv1.1 be disabled?

TLSv1.0 & TLSv1.1 support on Quickstream and WIBS will be disabled:

TEST Environment: **7th of December 2015**

PRODUCTION Environment: **18th of April 2016**

- **ccapi.qvalent.com – credit card API**
- **ws.qvalent.com – token requests**
- **ssiw.qvalent.com – WIBS file transfers via HTTPS or SOAP**

PRODUCTION Environment: **2nd May 2016**

- **quickstream.westpac.com.au – web browser access**
- **www.batchadvantage.qvalent.com – web browser access**
- **pnpnet.qvalent.com – web browser access**

1.5 How does disabling TLSv1.0 & TLSv1.1 affect my application?

When your application connects to one of the above URL's, it tells Qvalent's servers what protocol it would like to connect with, this will be either TLS 1.2, TLS 1.1 or TLS 1.0. Most modern software will connect using TLSv1.2. However if your application is using old software (such as Java 6) then it may only support TLSv1.0 or TLSv1.1. Once TLSv1.0 &TLSv1.1 is disabled then you will receive an error and will not be able to connect to the Qvalent application.

The same applies to accessing Qvalent websites using very old browsers that only support TLSv1.0 or TLSv1.1 (such as Internet Explorer 8). If you try and access a Qvalent website using a browser that only supports TLSv1.0 or TLSv1.1 after the cut-off date you will not be able to access the site and will receive an error.

1.6 What must I do?

If your application only supports TLSv1.0 or TLSv1.1 you will need to update your application to support at minimum TLS v1.2. If your browser only supports TLSv1.0 or TLS v1.1 you will need to update it to a newer version.

1.7 How do I know what protocols my application or browser supports

Westpac has been reviewing its logs attempting to identify all customers that are connecting via TLSv1.0 &TLSv1.1. Unfortunately this is a difficult task as Westpac only has an IP address to go off. For those customers that Westpac can identify, they will be contacted directly. However we cannot guarantee that all customers can be identified via this method. If you are unsure if your application supports TLSv1.2 Westpac strongly encourages you to test against the Westpac test environment (details below).

As a general guide, most product versions under vendor support will use TLSv1.2 or greater. For example, Oracle currently supports Java 8. However Java 6 and Java 7 are no longer supported. Java 8 supports TLSv1.2 while Java 6 does not. The same applies for web browsers, this however is much clearer cut. If your browser is currently supported by its vendor (such as Microsoft IE 11) then is will support TLSv1.2. While some products such as Java 7/IE9 can be configured to support TLS v1.2, Westpac would strongly recommend as good security practice to only use actively supported products.

1.8 How do I test my application or browser?

Westpac has an internet accessible test environment that mirrors production. Most customers would have used this environment when they were being implemented on the Quickstream or WIBS platform before going live. This test environment will have TLSv1.0 &TLSv1.1 disabled from 7th December 2015. If you can get a connection into this environment then you application or browser is using a minimum of TLSv1.2.

To test specific applications please use the following URL's:

QuickGateway

The URL you will use to connect depends on the programming environment that you are using:

a. If you are using a HTTPS Post to connect to the API, the URL is https://ccapi.client.support.qvalent.com/post/CreditCardAPIReceiver

b. If you are using SOAP to connect to the API, the URL is https://ccap.clienti.support.qvalent.com/webservice/CardsAPIDocumentLiteral

HTTPS File transfers

https://ws.support.qvalent.com or https://ssiw.support.qvalent.com depending on your production configuration.

Token Requests

To test token handoffs point your application to the test environment:

https://qsportal.atlassian.net/wiki/display/DOC/Notices

Web browsers

Point your web browser to the below URL. You will receive a message stating if you browser is TLSv1.2 compliant or not.

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

Additional information on browser support is available here:

https://qsportal.atlassian.net/wiki/display/DOC/Notices

2 FAQ's

2.1 I already performed work to disable the SSLv3 protocol in my application. Does this mean I am also ready for the TLSv1.0 disablement change?

No. Customers should not assume that the change performed previously to support the disablement of SSLv3 prepares their application for this change.

Customers should assess the capabilities of their software to use TLSv1.1 or higher to meet this requirement.

2.2 I use SFTP or XCom connectivity into WIBS. Am I impacted by this change?

Both the SFTP and XCom protocols do not use SSL as a channel encryption mechanism. There will be no change performed on these services.

2.3 Where can I find more information?

Please visit the following website:

https://qsportal.atlassian.net/wiki/display/DOC/Notices

3 Who do I contact if I need more information?

If you require further details or assistance, please contact your client enquiry manager or send the Quickstream Technical Help Desk an e-mail at quickstream@qvalent.com.