Westpac PayWay

Disabling TLSv1.0 & TLSv1.1

Date	Description
9/10/15	Initial Version
19/10/15	Updated
5/11/15	Revised
9/11/15	Revised
1/12/15	Revised
7/12/15	Revised
15/12/15	Revised
23/12/15	Revised for new PCI Council cut off dates

1 Disabling the TLSv1.0 & TLSv1.1 protocol

1.1 Who might this affect?

Businesses and/or individuals who use the PayWay API to process credit card transactions or requests a PayWay Net secure token for browser hand-off's to PayWay via HTTPS should read this document. This document is also relevant to customers who access the PayWay website via a web browser. The following URL's will be affected:

- **www.payway.com.au**

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 are used in all HTTPS communications between system to system or browser to system on the internet. TLSv1.0 was released in 1996. This was supplanted by TLS v1.1 in 1999. The most current version of TLS is 1.2 and was released in 2008.

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

The PCI council have deemed SSLv3 and early TLS are no longer considered strong cryptography and cannot be used as a security control after 30th June, 2016. Any organisation that has TLSv1.0 still enabled after this date will lose its PCI-DSS compliance. Many customers rely on Westpac and Qvalent to maintain this PCI compliance for their own certification.

For full details from the PCI council please refer to:

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

https://www.pcisecuritystandards.org/pdfs/15_12_18_SSL_Webinar_Press_Release_FINAL_%28002%29.pdf

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

TLSv1.0 support on PayWay will be disabled:

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

PRODUCTION Environment: **15th of April 2018**

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 PayWay'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 at TLSv1.2. However if your application is using an 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 the Qvalent application.

The same applies to accessing PayWay's website using very old browsers that only support TLSv1.0 or TLSv1.1 (such as Internet Explorer 8). If you try and access a PayWay 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 TLSv1.1 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 or 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 your application supports TLSv1.2 Westpac strongly encourages you to test against the Westpac browser 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?

If you are unsure if your application supports TLSv1.2 at a minimum, call the PayWay help desk (details below) and tell them the following information:

- Your public IP address
- The approximate time your application last accessed PayWay.

The PayWay help desk will look up your details to assist in determining if your application is still using TLSv1.0 or TLSv1.1.

Once you have made the necessary changes, please contact the PayWay help desk and they will assist in verifying those changes.

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://www.payway.com.au/core/BrowserTLSVersionView

Additional information on browser support is available here:

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

PayWay API

PayWay Net

To conduct a test PayWay Net transaction, send parameter **merchant_id** with a value of **TEST**. If your application is not TLSv1.2 complaint you will receive the following error:

```
TLS version TLSv1.0 is not strong encryption.  TLSv1.2 must be used.
```

PayWay Token Requests

To conduct a test PayWay Credit Card API transaction, send parameter **customer.merchant** with a value of **TEST**. If your application is not TLSv1.2 complaint you will receive the following error:

```
TLS version TLSv1.0 is not strong encryption.  TLSv1.2 must be used.
```

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 changes 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 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 the PayWay help desk:

PayWay Support on 1300 727 111 email: payway@qvalent.com

4 Disclaimer

These guidelines are general in nature and have been prepared without knowledge of the specific environment in which your systems operate. These guidelines are current at the time of writing, but may require update over time. They should not be forwarded to any other party without Westpac’s written consent. Except where contrary to law, Westpac intends by this notice, to exclude liability for these guidelines and the information contained in them. While Westpac has made every effort to ensure these guidelines are free from error, Westpac does not warrant their accuracy, adequacy or completeness.