# TLS 1.2 WEBINAR

## Everything Oracle Customers Need to Know

**Presented by Thomas McCullough**

Wednesday, September 13, 2017

cardconnect®
A First Data Company

# AGENDA

+ Overview of TLS
+ Customer Impact
+ TLS Versions/Examples
+ Oracle Impact + TLS 1.2 Enablement
+ Timeline of Activities
+ Q+A

# OVERVIEW OF TLS

## What is TLS?

Transport Layer Security

- The TLS protocol provides the key sharing mechanism to encrypt communications between two hosts
- The technology has been around since the 90's and has evolved over time
- SSL became TLS, but the name "SSL" is now a synonym to TLS

# SECURE COMMUNICATIONS ARE A MOVING TARGET

| Protocol | Availability | Status |
|---|---|---|
| SSL 3.0 | 1996 | Insecure |
| TLS 1.0 | 1999 | Insecure |
| TLS 1.1 | 2006 | Secure, but limited use |
| TLS 1.2 | 2008 | Secure |
| TLS 1.3 | 2017 | In Draft – Not yet released |

# OVERVIEW OF TLS

## Why is CardConnect making changes?

- The PCI (Payment Card Industry) Security Standards Council, which defines security and safety rules for the payments industry, no longer considers TLS 1.0 to be “strong cryptography” because it is vulnerable to various types of attacks.

- For additional information on TLS and and the risks that are present when using TLS version 1.0, please refer to the PCI Security Standards Council’s Information Supplement on Migrating from SSL and Early TLS.

# IMPACT TO YOU

## How is TLS Used at CardConnect?

- ALL web traffic to cardconnect.com sites are protected with TLS
- CardSecure Tokenizers
- Communications from a merchant's server to CardConnect's APIs
- Any time a client or server passes credentials
- Any time you connect to CardPointe or Copilot

# IMPACT TO YOU

- CardConnect API/Gateway
- CardSecure Tokenizer
- CardPointe and CoPilot Users
- Oracle E-Business Suite
- Web Browser Support

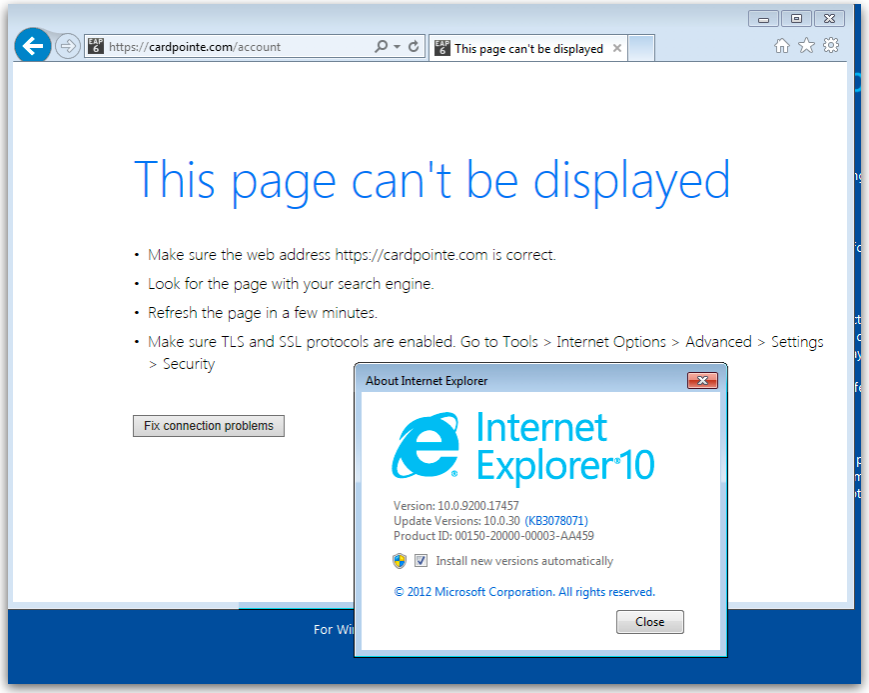
# OVERVIEW + BENEFITS

- Features Available with CardConnect Upgraded Code
  - Enhanced CardConnect Communication Security
  - Implementation Automation
  - Installation Checklist Report
  - CardConnect Web Tokenizer
  - CardConnect Card Validator
  - Account Updater Security and Performance Enhancements
  - Card Deposit Enhancements
  - End-to-End Payments transaction reporting
  - Post-Clone Port Update
  - Tax Exempt flag to allow L3 discounts for $0 tax transactions

- Support
  - https://support.cardconnect.com/security-resources/tls-1-2-upgrade
  - Assigned support resource
  - ERPSupport@cardconnect.com

# WHAT IS A HANDSHAKE FAILURE?

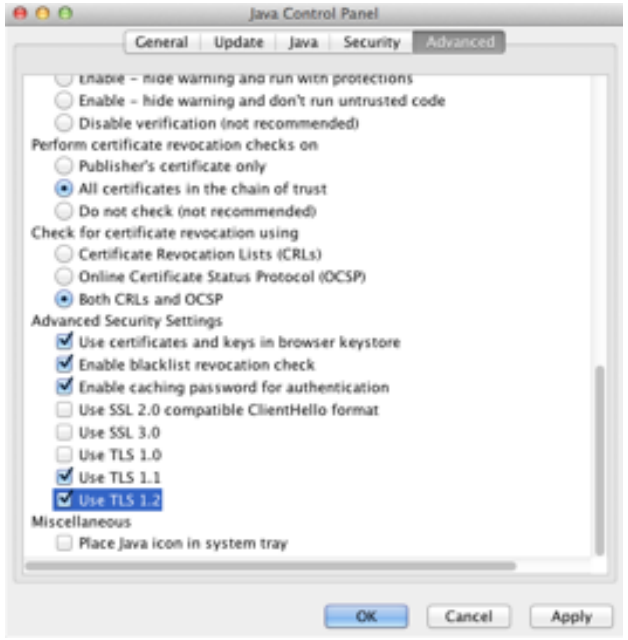
Handshake failures occur when both ends of a conversation cannot agree on how they will securely communicate.



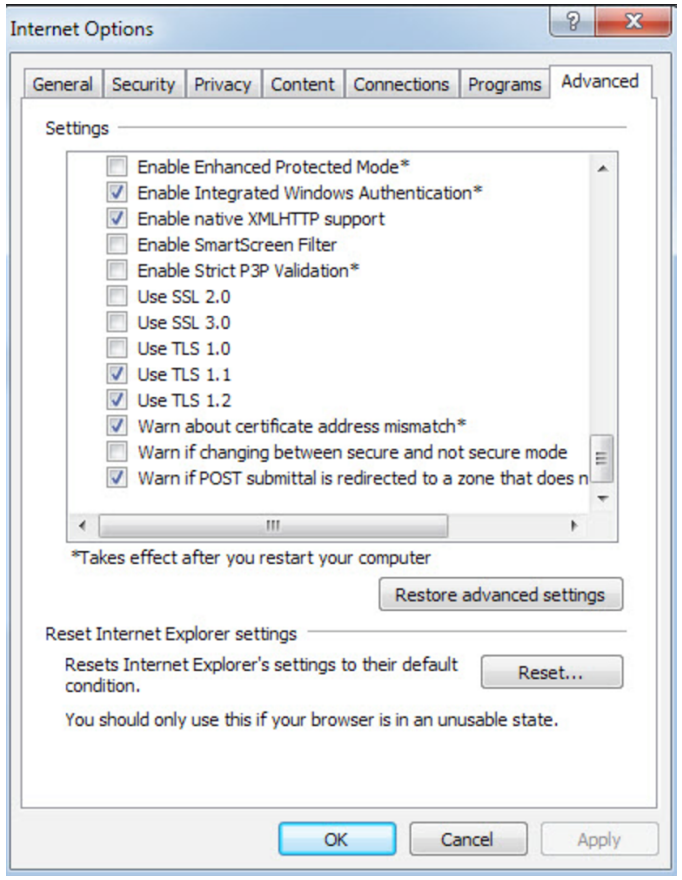

```
[jshipe /Users/jshipe ~]$ openssl s_client -ssl3 -connect www.cardpointe.com:443
CONNECTED(00000003)
14597:error:14094410:SSL routines:SSL3_READ_BYTES:sslv3 alert handshake failure:/BuildRoot
/s3_pkt.c:1145:SSL alert number 40
14597:error:1409E0E5:SSL routines:SSL3_WRITE_BYTES:ssl handshake failure:/BuildRoot/Librar
.c:566:
```

# ENABLING TLS 1.2 IN CLIENT SOFTWARE

## Enabling TLS 1.2 in Java 7




## Enabling TLS 1.2 in Internet Explorer



# API CONNECTION IMPACT - JAVA

- Java Support
  - If you run one of the following versions of Java, it is important that you take action before March 31st, 2018 to continue to communicate with CardConnect's services.

| Java Version | Details |
|---|---|
| JDK/JRE 7 Client | Yes, but support for TLS 1.2 must be enabled. |
| JDK/JRE 7 Server and Above | TLS 1.2 Enabled by default |
| JDK/JRE 6 and below | No TLS 1.2 support. |

- Support Site
  - https://support.cardconnect.com/security-resources/tls-1-2-upgrade#api-gateway-users

# API CONNECTION IMPACT - OPENSSL

- OpenSSL Support
  - Your OpenSSL version must be 1.0.1 or higher
- Common server platforms that depend on OpenSSL
  - Linux
  - Mac OS X
  - Node.js
  - Ruby
- Support Site
  - https://www.openssl.org/support/

# API CONNECTION IMPACT – ASP/.NET

- TLS Support varies based on your Windows Kernel
  - Uses a crypto library called Schannel

- Support Site
  - https://msdn.microsoft.com/en-us/library/aa380123(VS.85).aspx

# ENABLING TLS IN ORACLE EBS

- Steps to make necessary updates to TLS 1.2
  - Oracle Patching
  - Load balancer / F5 configuration
  - Ensure Minimum browser requirements

- Steps to Implement Additional Security Enhancements
  - Deploy CardConnect code as outlined in MD120
    - Recent implementation vs older implementations

- Recommended testing procedures
  - Provide the port 6443
  - Test connectivity during the UAT scheduled outages provided

# TIMELINE OF TESTING ACTIVITIES

| | |
|---|---|
| **October 16** | Testing – TLS 1.0 Traffic turned off in UAT |
| **November 13 – 15** | Testing – TLS 1.0 Traffic turned off in UAT |
| **December 4 – 6** | Testing – TLS 1.0 Traffic turned off in UAT |
| **January 22 – 24** | Testing – TLS 1.0 Traffic turned off in UAT |
| **February 19 – 21** | Testing – TLS 1.0 Traffic turned off in UAT |
| **March 31, 2018** | Testing – TLS 1.0 Traffic turned off in UAT and PRODUCTION |


Q + A


cardconnect®
A First Data Company