

For CitiDirect Users: Enabling TLS in Browser and Java settings

November 2014

Disclaimer:

In no event shall Citibank, N.A. and/or its affiliates ("Citi") be liable for any damages whatsoever, and in particular, Citi shall not be liable for special, indirect, consequential, or incidental damages, or damages for lost profits, loss of revenue, or loss of use, arising out of or related to any actions taken by you or your organization in reliance on the information in this message.

Table of Contents

Introduction	3
Background	3
What browser version do I have?	4
What Java version do I have?	5
Internet Explorer (IE) 8, 9 version	6
Internet Explorer (IE) 10, 11 version	7
MAC Safari	7
Java 7 and 8 Versions (1.7 Update xx and 1.8 Update xx)	8
Java 1.7.0_10 to latest Java version 1.8	8
Java 1.7.0_0 to 1.7.0_9	9
Java 6 Versions (1.6 Update xx)	10
Java 1.6.0_19 to 1.6.0_45	10
Java 1.6.0 to 1.6.0_18	11
Java 5 Versions (1.5 Update xx)	12
Java 1.5.0_22 to 1.5.0_28	12
Java 1.5.0_6 to 1.5.0_21	13
Java 1.5.0 to 1.5.0_04	13
Java 1.4	14
CitiDirect BE Mobile	15

Introduction

This document is intended for CitiDirect end users, and also IT security administrators as needed.

On **January 10, 2015**, a protocol known as Secure Sockets Layer version 3 (SSL 3.0) will be disabled on CitiDirect Web Servers. The information in this document provides guidance on how to ensure each user's computer is properly configured to run CitiDirect Online Banking and CitiDirect Services after SSL 3.0 is disabled on **January 10, 2015**.

On each user's computer, there are <u>two things that should be checked</u>: **Java setting** and **Browser setting**. To assist each individual user, this document provides the required steps for the Java and browser versions that we <u>currently</u> support.

Background

A weakness in the SSL 3.0 protocol was recently discovered and the attack that <u>demonstrates</u> this weakness is named **POODLE (Padding Oracle On Downgraded Legacy Encryption)**. The vulnerability is with the SSL 3.0 protocol itself and any web site or service that supports SSL 3.0 is exposed to being impacted by a POODLE attack.

Disabling SSL 3.0 in system/application configurations is the most viable solution to removing the POODLE vulnerability currently available – according to United States Computer Emergency Readiness Team (www.us-cert.gov/ncas/alerts/TA14-290A).

Transport Layer Security (TLS) is not impacted by this SSL 3.0 vulnerability and not subject to POODLE attacks. To avoid this vulnerability, the **TLS 1.0 protocol must be enabled in both your Browser and Java settings**. While all modern browsers and Java support the use of TLS, users can disable it in the settings of most browsers and Java. Thus, it is critical that you check your settings to ensure TLS 1.0 is enabled.

This issue has been assigned CVE-2014-3566. Common Vulnerabilities and Exposures (CVE[®]) is a dictionary of common names (i.e., CVE Identifiers) for publicly known information security vulnerabilities. More information about CVE can be found at:

https://cve.mitre.org/about/index.html

For Oracle's guidance on POODLE vulnerability, please click on this link: <u>http://www.oracle.com/technetwork/topics/security/poodlecve-2014-3566-2339408.html</u>

Again, the remediation for this SSL 3.0 issue is to disallow the use of SSL 3.0 and force the use of TLS on any web site or service where SSL 3.0 s in use. While all modern browsers and Java versions support the use of TLS, <u>users have the capability to turn it off in the settings on most browsers and Java</u>.

If a user's browser is configured to support <u>only</u> SSL 3.0 and they attempt to access a site where SSL 3.0 has been disabled, the browser will not be able to open a connection to the site.

What browser version do I have?

To determine the browser version currently installed on your computer see the steps below:

Internet Explorer

• Open Internet Explorer and navigate to Help menu \rightarrow About Internet Explorer



Based on the browser version installed, select the relevant link from the list below to view the actions required.

- Internet Explorer (IE) 8, 9
- Internet Explorer (IE) 10, 11
- MAC Safari

What Java version do I have?

To determine the Java version currently installed on your computer see the steps below:

• Open Internet Explorer and go to the following website: http://www.java.com/en/download/installed.jsp?detect=jre

If Java is correctly installed, it will display the current Java version on your computer similar to the screenshot below.



Based on the Java version installed, select the relevant link from the list below to view the actions required (applicable for both Windows and MAC operating systems)

- Java 1.5.0 to 1.5.0_04
- <u>Java 1.5.0_6 to 1.5.0_21</u>
- Java 1.5.0 22 to 1.5.0 28
- Java 1.6.0 to 1.6.0 18
- Java 1.6.0 19 to 1.6.0 45
- <u>Java 1.7.0 0 to 1.7.0 9</u>
- Java 1.7.0 10 to latest Java version 1.8

Note: Latest Java / Browser versions enable TLS 1.0 by default. However, it is recommended to check Java / Browser settings to make sure TLS 1.0 is enabled.

Internet Explorer (IE) 8, 9 version

- 1. Open "Internet Explorer" and click on "Tools" in the top menu bar of the IE browser
- 2. Click on "Internet Options"
- 3. Click on the "Advanced" tab within the Internet Options window
- 4. Scroll down in the "Advanced" tab and select "TLS 1.0" checkbox
- 5. Click "Apply" in the Internet Options tab

Internet Options		
General Security Privacy Content Connections Programs Advanced		
Settings		
 Enable DOM Storage Enable Integrated Windows Authentication* Enable memory protection to help mitigate online attacks* Enable smartScreen Filter Use SSL 2.0 Use SSL 3.0 Use TLS 1.0 Use TLS 1.1 Use TLS 1.1 Use TLS 1.2 Warn about certificate address mismatch* Warn if changing between secure and not secure mode Warn if POST submittal is redirected to a zone that does n 		
*Takes effect after you restart Internet Explorer		
Restore advanced settings		
Reset Internet Explorer settings Resets Internet Explorer's settings to their default Reset		
Condition. You should only use this if your browser is in an unusable state.		
OK Cancel Apply		

Internet Explorer (IE) 10, 11 version

- 1. Open "Internet Explorer" and click on "Tools" in the top menu bar of the IE browser
- 2. Click on "Internet Options"
- 3. Click on the "Advanced" tab within the Internet Options window
- 4. Scroll down in the "Advanced" tab and select "TLS 1.0" checkbox
- 5. Click "Apply" in the Internet Options tab



MAC Safari

No explicit setting change is required.

Java 7 and 8 Versions (1.7 Update xx and 1.8 Update xx)

Based on the minor version installed, the actions to be taken vary and are listed below:

Java 1.7.0_10 to latest Java version 1.8

- 1. Navigate to Java Control Panel
- 2. Click on the "Advanced" tab
- 3. Enable "TLS 1.0" checkbox under Advanced Security Settings and click "Apply" & "OK".

🛃 Java Control Panel	- • •
General Update Java Security Advanced	
Warn if site certificate does not match hostname	^
Show site certificate from server even if it is valid	
Mixed code (sandboxed vs. trusted) security verification	
Enable - show warning if needed	
Enable - hide warning and run with protections	
Enable - hide warning and don't run untrusted code	
Disable verification (not recommended)	
Perform certificate revocation checks on	
Publisher's certificate only	
 All certificates in the chain of trust 	
Do not check (not recommended)	
Check for certificate revocation using	
Certificate Revocation Lists (CRLs)	
Online Certificate Status Protocol (OCSP)	
Both CRLs and OCSP	
Advanced Security Settings	
Use certificates and keys in browser keystore	
Enable blacklist revocation check	
Use SSL 2.0 compatible ClientHello format	
Use SSL 3.0	=
Use TLS 1.1	
Use TLS 1.2	
Miscellaneous	
Place Java icon in system tray	
Suppress sponsor offers when installing or updating Java	-
OK Car	

Java 1.7.0_0 to 1.7.0_9

- 1. Navigate to Java Control Panel
- 2. Click on the "Advanced" tab
- 3. Navigate to Security \rightarrow General \rightarrow Enable "TLS 1.0" checkbox and click "Apply" & "OK".



Java 6 Versions (1.6 Update xx)

Java 1.6.0_19 to 1.6.0_45

- 1. Navigate to Java Control Panel
- 2. Click on the "Advanced" tab
- 3. Navigate to Security \rightarrow General \rightarrow Select "TLS 1.0" checkbox and click "Apply" & "OK".

🖆 Java Control Panel 📃 💷	×	
General Update Java Security Advanced		
	_	
I ⊕…Java Plug-in		
. Shortcut Creation		
Allow user to grant permissions to signed content		
Allow user to grant permissions to content from an untrusted autho	a l	
Use certificates and keys in browser keystore		
Use personal certificate automatically if only one matches server re	c	
Warn if site certificate does not match hostname		
	=	
Show sandbox warning banner		
Allow user to accept JNLP security requests		
Enable online certificate validation		
Enable blacklist revocation check		
Use SSL 2.0 compatible ClientHello format		
Use SSL 3.0	-	
OK Cancel Appl	y	

Java 1.6.0 to 1.6.0_18

- 1. Navigate to Java Control Panel
- 2. Click on the "Advanced" tab
- 3. Navigate to Security \rightarrow Select "TLS 1.0" checkbox and click "Apply" & "OK".

🖆 Java Control Panel 📃 💷	×	
General Update Java Security Advanced		
n in the in		
iter - Java Plug-In		
Allow user to grant permissions to signed content		
Allow user to grant permissions to content from an untrusted authority	,	
Use certificates and keys in browser keystore		
Use personal certificate automatically if only one matches server reques		
Warn if site certificate does not match hostname		
Show site certificate from server even if it is valid		
Show sandbox warning banner		
Enable online certificate validation		
Enable list of trusted publishers		
🔽 Enable blacklist revocation check		
Use SSL 2.0 compatible ClientHello format		
Use TIS 10		
Miscellaneous	-	
OK Cancel App	ly	

Java 5 Versions (1.5 Update xx)

Java 1.5.0_22 to 1.5.0_28

- 1. Navigate to Java Control Panel
- 2. Click on the "Advanced" tab
- 3. Navigate to Security \rightarrow Select "TLS 1.0" checkbox and click "Apply" & "OK".

👙 Java Control Panel 📃 🗖 🗖 🜌
General Update Java Security Advanced
Settings Debugging Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Settings Shortcut Creation Shortcut Creation Setting Settings
<u>OK</u> <u>Cancel</u> <u>Apply</u>

Java 1.5.0_6 to 1.5.0_21

- 1. Navigate to Java Control Panel
- 2. Click on the "Advanced" tab
- 3. Navigate to Security \rightarrow Select "TLS 1.0" checkbox and click "Apply" & "OK".



Java 1.5.0 to 1.5.0_04

There is no option to enable "TLS 1.0" for this Java version. Therefore, we **strongly recommend** upgrading to the latest version of Java.

In addition, all Java 1.5.x versions were removed from our list of CitiDirect-supported Java versions long ago.

Java 1.4

There is no option to enable "TLS 1.0" for this Java version. Therefore, we **strongly recommend** upgrading to the latest version of Java.

In addition, Java 1.4.x versions were removed from our list of CitiDirect-supported Java versions long ago.

Also, please note that public updates for these Java versions ended several years ago. See below from Oracle:

Major Release	General Availability Date	End of Public Updates
Java 4 (1.4.x)	February 2002	October 2008
Java 5 (1.5.x)	May 2004	October 2009

CitiDirect BE Mobile

For clients accessing CitiDirect BESM Mobile on their mobile device, please read below:

The Safari, Blackberry, and Internet Explorer <u>mobile browsers</u> all support TLS 1.0 by default, and should not require any additional changes. However, some older mobile phones may require an upgrade to a more recent mobile browser. When in doubt, please contact your IT Department or mobile phone providers for additional guidance and detailed instructions.